Volume 9
Issue 2
2022

NORTH EAST LAW REVIEW

LAW AND EMERGING TECHNOLOGIES

North East Law Review

2022

Volume 9, Issue 2: Special Issue on Law and Emerging Technologies

Newcastle University

The Editorial Board would like to thank all of the staff and students from Newcastle University who have helped in the creation of this issue. Without their support, the North East Law Review would not be possible.

This issue should be cited as (2022) 9(2) NELR

ISSN 2056-2918 (Print)

ISSN 2056-2926 (Online)

Newcastle University

NE1 7RU

Foreword by Professor Ben Farrand

I am delighted to be able to introduce this first special issue of the NELR, which focuses on topics of Law and Emerging Technologies. The focus of the special issue is one that is both understandable and welcome given developments at the Newcastle Law School over the past several years. As a School, we have seen a considerable expansion of our expertise in areas relating to technology broadly defined, complementing our existing strengths in subjects such as data protection, intellectual property, autonomous weapons systems and bioethics with colleagues working in fields such as cybersecurity, digital competition law, the regulation of Artificial Intelligence,[1] and the application of philosophical approaches to the reconceptualisation of our relations with other living creatures and their own legal status. This broad range of interdisciplinary interests is brought together in our Law & Futures research cluster, which reflects on the challenges we have, do, and will face, and how law can respond to these challenges in the future. Furthermore, we extend this expertise into our teaching, with our new LLM programme in Emerging Technologies and the Law, as well as the LLM in Competition Law and the Digital Economy that will begin running in the 2023 academic year. These programmes have a range of exciting modules that address these challenges, including regulatory responses to technological development and innovation, cybersecurity, social media regulation, the governance of digital competition and markets, and the laws applicable to AI.

In this respect, our research and teaching at Newcastle does not focus on 'emerging' technologies alone, but *issues* that are also emerging as we rethink our interactions with technology, or how technology shapes our interactions with each other. We have come quite a long way since the discussion about whether the revisiting of laws as a result of technological developments was really just a case of 'new wine in old bottles'.[2] As technologies, particularly the Internet, have become more widespread and pervasive in their use, the specificity of the problems they create, challenges they pose, and sometimes even the solutions they can bring,

[1] Which seems as good a place as any to state that this foreword was not written by Chat GPT, meaning any grammatical errors are unfortunately my own.

[2] Which started in disciplines such as management and technology studies in Alfred L Thimm, 'Old Wine In New Bottles? The Case of "Management Of Technology"' (1992) 4 Journal of Managerial Issues 210; Sam Ricketson, 'New Wine into Old Bottles: Technological Change and Intellectual Property Rights' (1992) 10 Prometheus 53; before being considered in law in DR Johnson and DG Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367.

have become subject to increased scrutiny. The interests of researchers rise and fall over time, with distinct waves of research into issues such as copyright enforcement online[3] and privacy and data protection[4] being some of the most obvious.

It is in the latest wave of technology-related interests that the articles in this special issue, being drawn from the excellent work of undergraduate, postgraduate taught and postgraduate research students from across the UK, fall – and what becomes immediately obvious is the increased focus on 'harm' in the context of the use and misuse of technologies. Ribera Martinez's opening article on steering end-user behaviour and Thomson's article on what the UK's Digital Markets Unit can learn from the EU's Digital Markets Act both consider the harms created by dominant market players skewing online behaviours through anti-competitive practices, demonstrating concerns with more economically oriented harms. Privacy remains a feature of online-facilitated harm research, with privacy concerns linked to the idea of 'competition justice' in Al Hinai's paper, while Gorecka considers whether privacy could be raised as a defence to an allegation of anti-competitive practices under Article 102TFEU. Privacy breaches feature as one of a number of potential harms in the articles by Yaxing Shi on private-public partnership and responsibility for cybersecurity provision, and Sooriyakumar on wearable devices, wearable medical devices, and product liability, which both raise questions as to what law can do to prevent misuses and abuses of data by considering the role of private sector operators in diverse sectors.

The final theme arising is the personal harms created by technologies being misused by individuals, such as the article by Phelan on the harms that must be addressed through the development of 'deepfake pornography' by AI systems and whether taking a responsible

[3] For example P Bernt Hugenholtz, 'Why the Copyright Directive Is Unimportant, and Possibly Invalid.' (2000) 11 European Intellectual Property Review 499; Giuseppe Mazziotti, *EU Digital Copyright Law and the End-User* (Springer 2008); Benjamin Farrand, 'Lobbying and Lawmaking in the European Union: The Development of Copyright Law and the Rejection of the Anti-Counterfeiting Trade Agreement' (2015) 35 Oxford Journal of Legal Studies 487; Severine Dusollier, 'The 2019 Directive on Copyright in the Digital Single Market: Some Progress, a Few Bad Choices, and an Overall Failed Ambition' (2020) 57 Common Market Law Review 979.
[4] Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1998); Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law & Security Review 509; Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 European Data Protection Law Review (EDPL) 28; Moritz Laurer and Timo Seidl, 'Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation' (2021) 13 Policy & Internet 257.

innovation approach can help to counter these harms, and McLaughlan's article on the physical and psychological harms caused by the spread of content promoting the use of anabolic steroids and other performance enhancing drugs through social media, and the extent to which this content can be tackled through regulatory initiatives such as the Online Safety Bill in the UK and Digital Services Act in the EU. These papers were very interesting to read and represent the formative ideas of a new generation of technology-focused scholars. I am once again very happy to have been involved in this process, and wish to extend my sincere thanks to the article writers, as well as Dr Ruth Houghton and Professor Oles Andriychuk for their outstanding work and efforts on this special issue, which would not have been possible otherwise.

North East Law Review Editorial Board 2022-2023

Academic Leads
Dr Ruth Houghton
Professor Oles Andriychuk
Professor Ben Farrand

Our thanks to the anonymous peer-reviewers.

The Editorial Board forms part of the broader project of the North East Law Review (NELR). The North East Law Review also includes the NELR Blog and the NELR podcast team.

This Special Issue has an accompanying blog piece written by Isaac Juma.

This year the NELR podcast was hosted by Scarlett Clarke, with editorial assistance by Daisy Robinson.

Contents Page

The Steering of End-User Behaviour in the Digital Markets Act: The Intrinsic Value of Trust for Governance

Alba Ribera Martínez

1. Introduction

The Digital Markets Act (DMA)[1] sets out the background and regulation applicable to the future designated gatekeepers who cater for core platform services. These gatekeepers, in the Commission's own words, have put digital markets at large and their relations with business and end users in the digital environment in jeopardy due to the presence of a lack of contestability and fairness. Although the former scenario has not been contested by scholars or practitioners due to past experience in the antitrust framework, the latter has sparked a myriad of reactions, stemming from the welcoming of the regulatory instrument to the outright dismissal of the DMA's founding objectives.

However, little attention has been granted to the benchmark against which the DMA's effectiveness should be assessed. It is unclear whether the regulatory instrument will have attained its objective once digital markets remain contestable and fair or once digital markets regain their competitive structure and conditions. In this same sense, the scholarly debate revolves around the DMA's prospects, whether they are purely deterministic -once a given competitive structure is restored in the digital arena, the provisions of the DMA do not apply to gatekeepers because their core platform services will subsequently fall out of the scope of the instrument- or stochastic in nature -the DMA will probably un-tip digital markets catering for core platform services with uncertain results-.

This latter possibility seems the closer one to the DMA's intentions, insofar as no material yardstick can be found throughout the DMA's text that would point towards a deterministic objective, i.e., the presence of *x* market players in the provision of core platform services *y* or

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

the possibility of conforming consumer choice into *n* choices from different economic operators. By this token, the regulatory instrument's purpose, in practice, is more difficult to grasp, especially when it comes to measuring its future effectiveness. However, this line of reasoning does not automatically imply that the DMA's goal is unattainable in terms of policy. Similar to other regulatory instruments, the DMA steers the behaviour of both its addressees (gatekeepers) and citizens at large (in economic terms, they would be identified with the role of end-users).

This article sets out the framework against which this steering process should be assessed in terms of its related consequences on the end-users, drawing some inspiration from the concepts of governance and trust. Although the DMA is yet in its early days when it comes to enforcement, the article sets out the adequate benchmark to measure the success of the application of its provisions, in line with the EU's desired broader policy objectives set out in its EU Digital Strategy.

2. The steering of end users: the feasible alternative for the digital market

Governance is nothing more (or less) than the measurement of a legislator's responsiveness towards citizens regarding the broader securement of the rule of law. In terms of the DMA, the rule of law has been finely disregarded in the digital sphere and should be reinforced through the wider purposes of securing contestable and fair digital markets. This yardstick to assess the interaction between the legislator and the citizens is normally characterised by three related elements: first, the source of the legislator's legitimacy, second, the capacity of the legislator to formulate and implement sound policies, and third, the responsiveness of the citizens (and the same legislator) regarding the norm as well as the economic and social interactions among them.[2]

[2] Christian Bjørnskov, 'How does social trust lead to better governance? An attempt to separate electoral and bureaucratic mechanisms' 2010). 144 Public Choice 323.

The article will grasp these elements to assess whether measuring the DMA's governance in the future is possible or not. Only if these elements are identified with particular benchmarks set out in the regulation, a satisfactory or unsatisfactory DMA governance may be outlined at a later stage of the instrument's implementation and enforcement. The deviations from these elements will tell whether the DMA is ill-conceived towards satisfying its fairness and contestability objectives or whether it is wisely articulated towards restoring an *ex-ante* foreground for the application of Articles 101 and 102 TFEU.

2.1 The DMA's legitimacy: a pending debate

In the case of the DMA, the insights of configuration theory are quite useful to overcome the theoretical complexity of spelling out each of these elements. Regarding legitimacy, from an institutional point of view, the DMA does not derive its efficacy from a directly appointed political institution designated through electoral democracy. Instead, the DMA was passed through a trilogue between the European Commission, the Council, and the European Parliament which set out the premises in which the DMA is founded: failure in competition law enforcement when it came to analysing practices taking place in the digital arena. The legal basis of the DMA, however, stems from a desire of the Union's institutions to unify the efforts to combat digital markets through a regulatory perspective under Article 114 TFEU.

As a reaction to the unpromising effects of competition policy when it came to digital markets, be that at the EU or national level, the Union steers the dynamics of digital markets from the realm of competition policy to the DMA. That is, the organisational aspect of the steering entity is now placed onto a regulatory instrument which has displaced the goals of antitrust for those of contestability and fairness. The legitimacy derived from Articles 101 and 102 TFEU is moved onto a regulation equally belonging to the realm of primary law with completely different objectives in mind. In this sense, Articles 5 through 7 of the DMA apply to digital gatekeepers to restore these particularly 'weak' digital markets up to their pre-tipping point stage.

This paradigmatical shift follows the structure of the traditional double-interact steering mechanism.[3] By this token, future behaviour is re-evaluated in light of previous experience: an action performed by an agent (act), triggers a second agent to respond (interact), which finally forces the first agent to re-consider the behaviour that was triggered. Translating double interact into the DMA, the European Commission and national competition authority's 'failed' -and segmented- enforcement in digital markets triggered the overall consensus that competition policy is not fit for curtailing the super-powers gained through 'tipped' digital markets and, thus, the EU re-considers shifting the steering process into a different instrument, i.e., the DMA.

The mechanism is coherent with the concept of market tipping that the DMA wants to address. In the past, tipping has been conflated with an economic model or a given mass of users that can predict the ignition of a domino effect on digital markets due to astronomical network effects built on top of digital platforms. However, the double interact-influenced steering process proposed by the DMA does not conflate the concept anymore. Instead, it perfectly aligns with the idea that tipping is more of a mental model characterising complex and recurrent behaviour patterns when user behaviour depends on the behaviour of other users. Nonetheless, measuring how un-tipped markets will look alike as a result of the DMA's enforcement will be quite complex, too, given its initial difficulty to estimate it.[4]

However, the digital *status quo* that the DMA wants to overcome is in itself quite contested from the perspective of the scholarly debate. Even though there is a preliminary agreement on the fact that digital markets pose a great challenge for competition authorities in terms of fact-searching and the conducting of investigations, a myriad of problems have been pointed out as the main cause for the European Commission's 'failure'. In this sense, the article only attends to those motives brought forward by the DMA.[5]

[3] Mark van Twist and C.J.A.M. Katrien Termeer, 'Introduction to Configuration Approach: A Process Theory for Societal Steering' in Roeland J. in t' Veld, Linze Schaap, C.J.A.M. Katrien Termeer and Mark van Twist (eds), *Autopoiesis and Configuration Theory: New Approaches to Societal Steering* (Kluwer Academic Publishers 1991).
[4] Nicolas Petit, *Big Tech and The Digital Economy: The Moligopoly Scenario* (OUP 2020).
[5] Digital Markets Act (n 1), Recital 5.

First, the lengthiness of sanctioning proceedings is highlighted throughout as one of the endemic reasons for competition policy's ineffectiveness when it comes to digital markets. Given that the anti-competitive practices and conducts take place in a developing and dynamic environment, once the competition authority concludes that there has been an infringement of competition law, the remedies for addressing the anti-competitive behaviour diminish in scope and size due to the fact that it might have evolved into a different behaviour into a related market or it might have vanished into thin air once enough time has passed since it was first implemented. The counterargument to this first reason is clear: ensuring that due process is safeguarded for the undertakings takes time. Therefore, anything contrary to ensuring the rights of defence and due process would run counter to the finding of an infringement. And second, sanctioning proceedings under Article 102 TFEU are only limited to certain instances of market power. Even in those cases where anti-competitive practices are captured under the lens of antitrust, the ensuring of a competitive process does not guarantee that fair economic outcomes are produced regarding core platform services. A similar counterargument applies here: competition law is characterised by its textured and open-ended provisions, but there is also a well-defined perimeter where unfair practices have not been correctly captured by the European Commission's prior enforcement of Article 102 TFEU and the subsequent case law. In the abstract, the DMA seeks to satisfy the enforcement gaps left by the application of Article 102(a) TFEU through the imposition of fair-er conducts in the form of prescriptions and prohibitions under Articles 5, 6 and 7 of the DMA.

Thus, the DMA takes recourse to a conflated approach towards the failure of enforcement in digital markets to build up its provisions on the basis of ending with fragmentation in the internal market through Article 114 TFEU. The failure that the DMA wants to end up with is not related to a particular understanding or functioning of competition law but to the multiplication of enforcement action throughout the Union in the form of rulemaking in the Member States to combat anti-competitive practices in national digital markets. This is the point where Article 114 TFEU comes in, and the source from which the DMA derives all of its legitimacy: the all-encompassing and ongoing objective to contribute to the proper functioning of the internal market by approximating diverging national laws which has survived throughout the different phases of the Union's integration since 1986.

However, the idea that Article 114 TFEU founds the DMA's legal basis is quite unpromising, insofar as fragmentation in the internal market due to diverging national laws and rules will still be the rule throughout the Member States. In this sense, the Greek, Austrian or German competition law amendments regarding digital markets is a primer for the general pattern: the DMA does not replace these amendments, nor they will be interpreted in the light of its provisions, given that the regulatory instrument falls out of the scope of Regulation 1/2003. Unsurprisingly, the DMA's legitimacy is quite controverted at the moment, from the perspective of effective governance ensuring its overall efficacy.

2.2 The implementation of sound policies: a trustworthy and fair digital environment

The DMA cannot be analysed in a vacuum, but next to the political normative preferences expressed by the Union throughout the last years regarding the EU Digital Strategy. In this respect, Vice-President Vestager's words encouraging the shaping of Europe's digital future to "*win people's trust and acceptance (by) (…) showing people that you accept the duties that come with being part of a society*" ring as true as ever. Likewise, in January 2023, the European Declaration on Digital Rights and Principles for the Digital Decade commits to provide access to a trustworthy, safe and secure digital environment based on fair competition. Thus, the purpose of securing fair competition is not strange to the general policy of the Union, although the DMA only defines unfairness with reference to the consequences inferred from an imbalance between the rights and obligations of business users where the gatekeeper obtains a disproportionate advantage (Recital 33).

From the perspective of assessing effective governance of the DMA is ensured, there is no immediate response as to how fairness could be measured regarding its impact on end-users. However, considering the broader picture, trust may be instrumentalised to test out the double interact paradigm. Up until this moment, end users have been satisfied with the range of choices and services catered for them for free (act), which has led digital companies to profit from that situation for their own benefit through their exploitation (interact). For instance, digital platforms have exploited end user's personal data throughout their activities. Hence, end users

must reconsider their prominent position within the digital arena and make businesses liable for their conduct (double interact).

Not only fairness but trust is also assigned a prominent role in the transformation of the dynamics of digital markets. Due to its inherently anthropomorphic form, trust has been seldom instrumentalised in the context of economic exchange, although some attempts to capture the phenomenon were first sketched out in transaction cost economics as well as in the field of economic sociology.[6] Even though the organisation and strategy literature has asserted that trust in economic exchange is beneficial and can be a source of competitive advantage due to its resonance with efficient governance, these assumptions have not yet been translated into the digital arena or towards the broader spectrum of the user before digital platforms.[7] The need for addressing the lack of contestability and fairness in digital markets is commended as the objective fact on which the DMA is cemented, although its legitimacy is not based on these goals.

Given that the burden of mistrust is placed on the gatekeeper, the burden of intervention to comply with the obligations laid down in Articles 5, 6 and 7 of the DMA is also allocated to the gatekeeper through the introduction of a compliance function (Article 28 of the DMA). The effective compliance of these provisions cannot be undermined by "*any behaviour*" performed by the gatekeeper, regardless of whether that "*behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design"* (Article 13(4) of the DMA). In this sense, trust is projected not as an expected reality produced by the DMA's provisions, but as an expectation of the gatekeeper's future behaviour due to the uncertain anticipation of how the DMA's rules will apply.

Although compliance by design is expected, the DMA does not tailor each gatekeeper's business model to a one-size-fits-all solution. Instead, it imposes obligations and prescriptions

[6] Oliver Eaton Williamson, *The Economic Institutions of Capitalism* (The Free Press, 1985); Robin Dore, 'Goodwill and the Spirit of Market Capitalism' (1983) 34 British Journal of Sociology 459.
[7] Kenneth Arrow, *The Limits of Organizations* (Norton 1974); Philip Bromiley and Larry L. Cummings, 'Transaction Costs in Organizations with Trust' in Roy J. Lewici, Robert J. Bies and Blair H. Sheppard (eds), *Research on Negotiation in Organizations* (Elsevier Science/JAI Press 1974).

that the addressee: (i) is relied on to fulfil -under the looming danger of being applied the non-compliance fines set out in Article 30 of the DMA-; (ii) in a predictable manner and, in this context, (iii) the gatekeeper is expected to act and negotiate fairly when the possibility of deviating is presented. In short, the gatekeepers are not 'entrusted' with the DMA's compliance, but they are 'expected' to avoid betraying end users' trust once again.[8]

Having said that, the European Commission's monitoring of the gatekeeper's compliance acts as a supervisory agent ensuring that relational trust flows both ways (gatekeepers-users) as well as with its own agents (gatekeepers-EC). The main instrument to ensure trust is strengthened throughout the DMA is the possibility of performing market investigations when monitoring the compliance of the rules of the DMA. That is, the EC may take a snapshot of the "*broader contestability trends in the digital sector*" to ensure that non-compliance does not crystallise into betrayal of business and user trust through the investigation of systematic non-compliance.

In any case, the facilitation of the interaction process for the steering of end users into trusting (again) the economic operator in the digital arena is not devised with a set of concrete values in mind. Instead, it is outlined through the translation of un-values to the legal sphere.[9] That is, past experience has shown what ought not to be done, and the ethical space of the regulatory instrument is thus sketched out. By doing this, the Union sets out a sphere of action correlated with the current state of things: the Union does not wish to maintain the digital arena and the interactions therein as it is, and it ought to change.

All in all, the Union's capacity to devise an adequate instrument in line with its sound policies depends on a relatively open-ended and textured understanding of the digital market based on an intuitive benchmark. If digital markets do not look alike the way they do now, they should at least be trustworthy because they align with the DMA's interests. Moreover, in those instances where they do look alike to the existing panorama, then antitrust rules may be applied -with the intrinsic risks for failure looming over the competition authority- or the speedy non-

[8] Akbar Zaheer, Bill McEvily and Vincenzo Perrone, 'Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance' (1998) 9 Organization Science 141.
[9] The concept of un-values stems from Mark van Twist and C.J.A.M. Katrien Termeer, 'Introduction to Configuration Approach: A Process Theory for Societal Steering' (n 3) p. 26.

compliance procedure may be triggered to compel the gatekeeper's behaviour into compliance of the DMA's prescriptions and prohibitions.

2.3 Responsiveness of end-users before the DMA

Even though the DMA is particularly addressed to digital operators catering for core platform services through its provisions, end-users have a key role to play when it comes to assessing whether the DMA's effective governance is even possible. The steering process towards the alignment of end-user behaviour with the interests pursued by the Union begins by equating trustworthiness to accountability, and this last process can only be measured against the citizen/user's responsiveness towards the DMA.

Responsiveness may be measured in a negative or a positive light. On one side, the negative implications of equating trust with accountability at the end-user side imply that they have to be coherent and consistent with the choices they make online regarding core platform services. This is, they must punish the deviations performed by gatekeepers from the prescriptions of the DMA, be that through a lenient or harsher understanding of the punishment. On the other side, positive consequences inferred from the recoupment of end-user trust entail that when the end-user perceives that a gatekeeper is compliant with the DMA's provisions it should reward the economic operator in some way. For example, the end-user may make a core platform service provider a default in her daily use of services because he has demonstrated a compliant attitude towards the norm. These inferences, however, are unrealistic: they assume the lack of existence of asymmetries of information, a fully-fledged knowledge of the DMA's provisions and each of the gatekeeper's degree of compliance over them as well as their capacity to switch, multi-home and opt-out of core platform services without bearing switching costs by doing that. Ironically, most of the problems impeding end-user accountability today will potentially be eliminated by the enforcement of the DMA in the future.

Past experience has shown that end-users do not care or do not proactively react to the lack of compliance of other norms which have been in force for quite some time. For instance, the consequent infringements adverted by data supervisory authorities performed by digital

companies (at times, against the same economic operators who are expected to be designated as gatekeepers) have not discouraged end-users to continue opting in into sharing their personal data for unlawful legal basis under the GDPR.

Hopefully, the double interact motion will be triggered with time regarding the DMA and end-users will make digital platforms accountable for their actions. In line with the timeframes used in social steering, this endeavour will conceivably crystallise in the long-term and, perhaps, in a completely different digital background that will need from a distinct end-user reaction towards digital economic operators.

3. Conclusions

The Digital Markets Act steers the future designated gatekeeper's conduct in the particular direction of the prescriptions and provisions of Articles 5, 6 and 7, whereas it is also intended to steer end-user behaviour in two related ways. First, the Union's overall digital strategy is aimed to create a trustworthy digital environment. In this stage of the DMA's entry into force, the steering process has thus begun. Second, the Union's efforts are also directed to steer end users by instrumentalising trustworthiness into accountability. In other words, if gatekeepers deviate from unfair behaviour, they should be held accountable.

Steering in any form, especially when it comes to influencing and administering the interests of citizens, does not always produce the intended outcomes that a legal norm seeks to attain. This article has set out preliminary benchmarks which may be used in the future to assess whether the DMA is governed according to its objectives or not. Concerning legitimacy, fragmentation should be averted as the first hurdle to be overcome by the regulatory instrument, although the DMA may produce its related outcomes in a fragmented internal market. This would infer the failure of utilising Article 114 TFEU against its own nature. In terms of the implementation of a sound policy, the DMA replaces the textured provisions of Articles 101 and 102 TFEU for the open-ended concepts of fairness and trust, that is, at least, in line with the EU's broader policy objectives. Coherence is secured, although the measurement of fairness and trust, especially when it comes to assessing the citizens' responsiveness towards

the instrument, come short of being particularly informed with behavioural preferences and the long-term processes of social steering.

Are the Current Legal Responses to Artificial Intelligence Facilitated 'Deepfake' Pornography Sufficient to Curtail the Inflicted Harm?

Patrick Phelan

1. Introduction

Although artificial intelligence (AI) has created new opportunities, it has revolutionised how sexual violence can be inflicted. Furthermore, the ubiquity of smartphones and internet accessibility means image-based sexual abuse (IBSA) is perpetuated online.[1] Virtual revenge pornography is no longer a dystopian concept, but a present-day threat.[2] In examining 'deepfake pornography', this article highlights its threat to individuals, namely women, by eroding their sexual autonomy. Although much literature focuses on deepfake content causing societal damage to national security and democratic institutions, this article concentrates on pornographic harm.[3] The ensuing part explains how deepfake works and its applicability to pornography, followed by explaining why it perpetuates sexual violence. This article will then highlight legal challenges involved in regulating deepfake pornography, before exploring legal avenues to be pursued for harm mitigation, without stifling AI innovation.

2. AI and pornography

Named after its technological foundation, 'deepfakes' operate through 'deep learning algorithms.'[4] Combined with the capacity to handle multi-layer neural networks, thousands of

[1] Miha Sepec and Melanija Lango, 'Virtual Revenge Pornography as a New Online Threat to Sexual Integrity' (2020) 15 *Balkan Social Science Review*, 117, 129.
[2] Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37(3) *Oxford Journal of Legal Studies*, 534, 534-535.
[3] Matthew B. Kugler and Carly Pace, 'Deepfake Privacy: Attitudes and Regulation' (2021) 116 *Northwestern University Law Review* 611, 623 ; Konstantin A. Pantserev, '*The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability*' in Hamid Jahankhani, Stefan Kendzierskyj, Nishan Chelvachandran and Jaime Ibarra (eds) '*Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*' (first published 2020, Springer) ; Erkam Temir, 'Deepfake: New Era in The Age of Disinformation & End of Reliable Journalism' (2020) 13(2) *Journal of Selcuk Communication* 1009-1024.
[4] Dave Johnson, 'What is a deepfake? Everything you need to know about the AI-powered fake media' (*Insider*, 10 August 2022) < https://www.businessinsider.com/guides/tech/what-is-deepfake?r=US&IR=T#:~:text=The%20term%20%22deepfake%22%20comes%20from,make%20realistic%2Dlooking%20fake%20media.> accessed 6 November 2022.

images can be processed at once.[5] Consequently, female celebrities can find themselves in videos with a combined view count of over 134 million across popular deepfake pornography websites.[6] AI analyses their images and prepares an algorithm which formulates how that person's facial expressions would have to appear in order for augmented content to mimic realistically.[7] An 'autoencoder' uses an encoder to reduce the image to a lower-dimensional latent form, and a decoder which then reconstructs an image from the latent form.[8] The fabricated representation is then upgraded using 'generative adversarial networks' (GANs) which train the discriminator with the decoder "in an adversarial relationship, creating new images from the latent representation."[9]

As GANs enable continuous improvement to generated footage, this aggravates pornographic harm.[10] When giveaway characteristics of deepfakes are exposed, developers now have material to feed back to the discriminator, allowing the refinement of identified defects.[11] Previously, giveaway characteristics ranged from poor lip-synching, to badly rendered hair, jewellery and teeth.[12] However, pairs of algorithms will continue to be "pitted against each other", contributing to ever-increasing realism.[13] Furthermore, in recent years deepfake software has become widely available to the public whereas previously it was only accessible for those who could afford it.[14] With tutorials available online, deepfakes can be created "from the comfort of one's own home with relative ease."[15] Thus, individuals perpetuate IBSA by taking advantage of what Kastleman describes as the 'four A's' of internet pornography: accessibility, affordability, anonymity, and aggression.[16]

---

[5] Madhura Thombre, 'Deconstructing Deepfake: Tracking Legal Implications and Challenges' (2021) 4(2) *International Journal of Law Management & Humanities* 2267, 2268.
[6] Henry Ajder, Giorgio Patrini, Francesco Cavalli and Laurence Cullen, 'The State of Deepfakes' (*Deeptrace*, September 2019) <https://regmedia.co.uk/2019/10/08/deepfake_report.pdf> accessed 7 December 2022.
[7] Thombre (n 5), page 2268.
[8] Yuru Lin and Krishnaveni Parvataneni, 'Deepfake Generation, Detection, and UseCases:A Review Paper' (2021) 3(2) International Journal of Computational and Biological Intelligent Systems 1.
[9] Ibid.
[10] Adrienne de Ruiter, 'The Distinct Wrong of Deepfakes' (2021) 3 *Philosophy & Technology* 1311, 1315.
[11] Ibid.
[12] Ian Sample, 'What are deepfakes – and how can you spot them?' (*The Guardian*, 13 January 2020) <https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them> accessed 7 December 2022.
[13] Sepec and Lango (n 1), 119.
[14] James Linen, 'How Fabricated Videos Are Being Used To Harm Women' (*GenxNews*, 28 September 2022) < https://genxnewz.com/how-fabricated-videos-are-being-used-to-harm-women/> accessed 7 December 2022.
[15] Sepec and Lango (n 13), 120.
[16] Mark B. Kastleman, '*The Drug of the New Millennium - The Brain Science Behind Internet Pornography Use*' (first published 2001, Granite Publishing and Distribution).

3. Consequential harms

3.1 Accessibility

There are many parallels between deepfake pornography and 'revenge porn', defined as the non-consensual sharing of private, sexual materials of another person with the intent to cause embarrassment or distress.[17] Accessibility is mirrored between both revenge and deepfake pornography as a simple search will produce relevant results. Although pornography websites attempt to ban deepfakes, Maddocks found that two large companies still featured 'deepnude' content as of January 2020.[18] Deepfake content remains online due to lacklustre attempts to fight it, epitomised in Pornhub's effort to remove videos titled 'deepfakes' but not 'deep fakes' or 'deepfake.'[19] Major pornography websites have been exposed in the past for promoting sexual violence, including 'revenge porn', 'upskirting', and voyeurism.[20] It is therefore no surprise that pornography companies are trying to profit from non-consensual deepfake pornography.

3.2 Affordability

Deepfake pornography is viewed by Gieseke as "the next iteration of revenge pornography" since perpetrators can obtain videos starring any woman they have photos of, rather than anticipating nude images to be leaked online.[21] Illustrated by Rini and Cohen, perpetrators can chose the individual to be swapped into particular sex acts as casual as "ordering toppings on

[17] Ministry of Justice, 'Revenge Porn: The Facts' (GOV.UK, 2015) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf> accessed 7 December 2022, page 1.
[18] Sophie Maddocks, '''A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political' deep fakes' (2020) 7(4) *Porn Studies* 415, 417.
[19] Ibid.
[20] Fiona Vera-Gray, Clare McGlynn, Ibad Kureshi and Kate Butterby, 'Sexual violence as a sexual script in mainstream online pornography' (2021) 61(5) *The British Journal of Criminology* 1243, 1249 to 1251.
[21] Anne Pechenik Gieseke, '"The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography' (2020) 73 *Vanderbilt Law Review* 1479, 1481.

a pizza."[22] Creation is cheap, demonstrated by 'Deepfakes Web' charging $15 and $60 respectively for basic or high-quality content.[23] With prices and efforts low for perpetrators, opportunities are there to sell content. This parallels 'revenge porn' where perpetrators can charge as little as £5 for a victim's nude images.[24] This commodification incentivises pornography companies to create and sell deepfake content, and for individuals to offer their services.[25]

3.3 Anonymity

With 'revenge porn', Kamal and Newman explain how anonymity is an obstacle in the avenue to redress as it can be difficult to identify the individual responsible.[26] This issue is exasperated with deepfake pornography since there is no original photo that can be traced to anyone. Instead, photos of celebrities can be obtained via the internet and photos of private individuals through social media. Using the "perk of anonymity", Rosewarne is not surprised that the same misogyny plaguing the offline world is materialising on a larger scale online as the internet makes it easier to do.[27] Using images of someone for deepfake pornography is not only a clear invasion of privacy, but also personal and sexual integrity.[28] As GANs enable consistent improvement of video, the line between real and fake dissolves. Deepfake pornography will appear real; celebrities may be able to get away with saying that such videos are fake, but private individuals will not be afforded this luxury. As it is impossible to be familiar with the face of someone you do not know, it will consequently be impossible for viewers to ascertain that the 'person' featured did not actually take part. Perpetrators can hide behind anonymity and use AI to turn someone's sexual privacy into another person's reality.

---

[22] Regina Rini & Leah Cohen, 'Deepfakes, Deep Harms' (2022) 22(2) *Journal of Ethics and Social Philosophy*143, 146.
[23] Deepfakes Web, 'Make Your Own Deepfake! [Online App]' (*Deepfakes Web*) <https://deepfakesweb.com/> accessed 8 December 2022.
[24] Monika Plaha and Panorama team, 'Inside the secret world of trading nudes' (*BBC News*, 22 August 2022) < https://www.bbc.co.uk/news/uk-62564028> accessed 8 December 2022.
[25] Gieseke (n 21), 1485.
[26] Mudasir Kamal and William J. Newman, 'Revenge Pornography: Mental Health Implications and Related Legislation' (2016) 44(3) *Journal of the American Academy of Psychiatry and the Law* 359, 363.
[27] Lauren Rosewarne, '*Abuse as Artefact: Understanding Digital Abuse of Women as Cultural Informant*' in Anastasia Powell, Asher Flynn and Lisa Sugiura (eds) 'The Palgrave Handbook of Gendered Violence and Technology' (first published 2021, Palgrave MacMillan) 135, 149.
[28] Sepec and Lango (n 15), 119.

3.4 Aggression

While self-gratification seems to be the main purpose of pornographic deepfakes, they have the potential to be used to extort, humiliate, and blackmail.[29] As deepfakes give creators a form of power over others by making them perform acts they may otherwise not consent to, this leads to pornographic misuse.[30] Deepfake, according to Rosewarne, is inherently gendered and a reflection of the "very worst of patriarchy and the power disparities" between men and women.[31] Similarly, Citron and Franks conclude that undermining women's autonomy through IBSA relates to the "idiosyncratic, dangerous views about consent with regard to sex."[32] Sadly, the central theme for online IBSA is the removal of consent. Through deepfake pornography, women's autonomy is eroded further. Although deepfake pornography is not real, individuals are still reduced to "genitalia, breasts, buttocks, and anuses" by creators, accused by Citron of hijacking sexual identities and exercising dominion over stolen sexualities by exhibiting it to others.[33]

4. Legal challenges

4.1 Criminal and tort law failures

Regulating deepfake pornography by analogy to revenge pornography can create problems. Revenge pornography is governed by section 33 of the Criminal Justice and Courts Act 2015 (CJCA), creating an offence where a person discloses a private sexual photograph or film, without consent, with an intention to cause distress.[34] However, this wording has created a disastrous lacuna as the mens rea element of the offence is narrow, only catching perpetrators

[29] Douglas Harris, 'Deepfakes: False Pornography Is Here and the Law Cannot Protect You' (2018-2019) 17 *Duke Law & Technology Review* 99,102.
[30] Rini and Cohen (n 22), 145.
[31] Rosewarne (n 27), 149.
[32] Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn' (2014) 49(1) *Wake Forest Law Review* 345, 348.
[33] Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *The Yale Law Journal* 1870, 1921.
[34] Criminal Justice and Courts Act 2015 (CJCA), section 33.

with an intent to cause distress. As McGlynn and Rackley highlight, dissemination may be encouraged by financial gain, amusement, or sexual gratification.[35] If the legal response to revenge pornography is not suitable for the offence it tries to curtail, it will not have much success in preventing deepfake pornography either. Attempting to govern deepfake pornography by analogy displays a 'Law 1.0' attitude, whereby existing rules, standards, and general principles are applied to particular fact situations.[36] However, as Brownsword explains, pressure increases on a Law 1.0 approach when society industrialises through technology because existing law is not "geared to respond to the range of risks that now present themselves."[37] When the CJCA was drafted, deepfake pornography was not conceivable. As it develops and becomes increasingly harmful by the video, it would be stubborn for lawmakers to regulate through a faulty legal response.

Furthermore, attempting to remedy deepfake pornography through tort law raises questions of accuracy. Established in *Campbell*, it was held that a breach of confidence would arise when material of a private nature was disclosed, being "highly offensive to a reasonable person of ordinary sensibilities."[38] Although the reasonable person of ordinary sensibilities may view deepfake pornography as offensive, the issue is that no breach of confidence has occurred. As AI generates a fake video of an individual, no actual footage has been disclosed. Likewise, the test laid out by Justice Meggary to determine breach of confidence in *Coco* is not relevant to deepfake pornography.[39] A claim would succeed where the disclosed information has the necessary quality of confidence, was communicated with an implied obligation of confidence, and lead to an unauthorised use of that information to the detriment of the party communicating it.[40] However, deepfake pornography creates a situation where content is produced without any initial disclosure, therefore no breach of confidence has occurred, despite harm being inflicted on a victim who did not communicate anything in the first place. Furthermore, *Mosley* established the principle that those involved in sexual relationships "may be expected not to reveal private conversations or activities."[41] However, victims of deepfake pornography now do not even have to engage in sexual activity to be targeted. Private conversations and activities

[35] McGylnn and Rackley (n 2), 555.
[36] Rodger Brownsword, '*Law 3.0: Rules, Regulation, and Technology*' (first published 2020, Routledge), 3.
[37] Ibid.
[38] *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22, paragraph 166.
[39] *Coco v AN Clark (Engineers) Ltd* [1968] F.S.R. 415.
[40] Ibid, at 419.
[41] *Mosley v News Group Newspapers Ltd* [2008] E.M.L.R. 20, at 105.

are no longer revealed – deepfake pornography can create them. Thus, leading tort law authorities are redundant. Without addressing this, courts will face increased pressure to bend statutes to protect deepfake pornography victims, considering how tort doctrines and revenge pornography statutes were not drafted with the consequences of a technology that "transforms a person's sexual fantasy into reality" in mind.[42]

4.2 Pervert's rights?

Another challenge for lawmakers when approaching deepfake pornography is whether to adhere to the "normative equivalency paradigm" which ensures that rights enjoyed by individuals offline are protected online.[43] Although personal deepfake pornography may be "lewd and even despicable", Harris is aware that they do not perpetuate the same harms since moral disapproval cannot justify illegality.[44] Introducing 'the Pervert's Dilemma', Öhman describes the situation where: (i) creating deepfake pornography, without the individual's consent is morally impermissible; (ii) having private sexual fantasies about someone, without their consent, is per se normally morally permissible; (iii) therefore, based on (i) and (ii), "there is no morally relevant difference" between creating deepfake pornography and having a private sexual fantasy.[45] There are no laws which criminalise sexual fantasy as this would not be proportionate under freedom of expression protected in Article 10 of the Human Rights Act.[46] Furthermore, if the 'pervert' has a right offline, it is interesting to consider whether this should be upheld online. Kettemann and Benedek argue that freedom of expression on the internet should extend to irrational discourse, including content which may "shock, offend, or disturb."[47] Applying this to deepfake pornography, creators should be allowed to share their deepfake pornography online as sexual expression should also be protected.

---

[42] Harris (n 29), 128.
[43] Dafna Dror-Shpoliansky and Yuval Shany, 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology'(2021) 32(4) *The European Journal of International Law* 1249, 1281.
[44] Harris (n 42), 125.
[45] Carl Öhman, 'Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2019) 22 *Ethics and Information Technology* 133, 134.
[46] Human Rights Act 1998, Article 10.
[47] Matthias C. Kettemann and Wolfgang Benedek, '*Human Rights, Digital Society and the Law*' (first published 2019, Routledge), 74.

5. Legislative response

5.1 Legislative updates

Rather than relying on section 33 CJCA to catch perpetrators who created deepfake pornography to cause distress, recommendations by the Law Commission should be enshrined within law reform. Considering the concerns regarding personal creation, the Law Commission understands that criminalising 'making' would be problematic to enforce and recognises that harm arises from sharing.[48] Despite the previous view of Kettemann and Benedek, allowing deepfake pornography online would permit IBSA. As Maddocks recommends, policy makers should "seek to challenge the longstanding inequalities that lead AI to disproportionately target women."[49] Thus, lawmakers should reform section 35(5) CJCA[50] to include images made intimate through alteration as this provision extends to how section 33 CJCA is applied.[51] This decision to adapt the law is welcomed as this resembles 'Law 2.0', explained by Brownsword as the articulation of new rules and regulatory frameworks.[52]

As online harm becomes increasingly prevalent, the government announced the Online Safety Bill (OSB).[53] Under Section 9(3) OSB, duties of care are placed on website providers to minimise the presence of 'priority illegal content', the length of time it is present on the service, and its dissemination.[54] Also, when the website is alerted about illegal content, they must remove such content swiftly.[55] Although section 33 CJCA is included as priority illegal content, this does not extend beyond the current scope of the law, meaning deepfake pornography would not be caught.[56] Therefore, if section 33 CJCA is reformed to criminalise deepfake pornography, websites would be required to be proactive in removing AI-enabled IBSA.[57] Under section 85(4) OSB, pornography websites that do not adhere to their new duties can be

[48] Law Commission, '*Intimate Image Abuse: A Final Report'*, (Law Com No 407, 2022), 157.
[49] Maddocks (n 18), 420.
[50] CJCA, section 35(5).
[51] Law Commission (n 48), 163.
[52] Brownsword (n 37).
[53] Draft Online Safety Bill (2021, CP 405).
[54] OSB, section 9(3)(a) to (c).
[55] Ibid, section 9(3)(d).
[56] Ibid, Sch 7, para 26.
[57] Law Commission (n 51), 422.

fined up to £18 million or 10% of their annual global turnover.[58] Considering tort law has influenced the inclusion of duties of care into the online world, civil claims may be worth exploring as a remedy to deepfake pornography. By introducing a new civil offence, victims are given avenues of support and redress beyond criminal law, while tackling online dissemination by targeting hosts of ISBA and individuals sharing images without consent.[59] In support, the Angelou Centre and Imkaan assert how additional civil avenues should be available for victims who do not wish to pursue action through the criminal justice system as "it is not an equitable system, particularly for black and minoritised women and children victim-survivors."[60]

5.2 Responsible innovation

Deepfakes can be viewed as morally problematic as they possess significant potential to deceive.[61] However, as Thombre explains, a complete ban on deepfakes can have chilling effect on free speech.[62] It is therefore crucial when legislating deepfake pornography that criminalisation is focused on the infliction of harm against victims, rather than preventing deepfake to be used at all. The defendant argued in *Anzalone,* an American case regarding a child pornography website, that the government epitomised "outrageous conduct" after seizing and overseeing the website for two weeks, thus perpetuating child abuse.[63] Considering this, Olson ponders whether synthetic materials, such as AI, can be used in future, rather than using real images of children. [64] In the past, a similar idea was demonstrated in 'Sweetie', a computer-generated image of a 10-year-old child to catch predators online.[65] 'Sweetie's' success implies that AI could create indistinguishable versions of child pornography to catch predators without

[58] Ibid, section 85(4).
[59] Clare McGlynn and Erika Rackley, 'Intimate Image Abuse – Policy Briefing on Law Commission Consultation' (5 May 2021) < https://claremcglynn.files.wordpress.com/2021/05/mcglynnrackley-stakeholder-briefing-5-may-2021-final.pdf> accessed 10 December 2022.
[60] Law Commission (n 57), 418.
[61] De Ruiter (n 10), 1321.
[62] Thombre (n 7), 2274.
[63] *United States v. Anzalone*, No. 17-1454 (1st Cir. 2019), page 9.
[64] Abigail Olson, 'The Double-Side of Deepfakes: Obstacles and Assets in the Fight against Child Pornography' (2022) *Georgia Law Review*, 56, 865, 885.
[65] Leslie Katz, 'Meet 'Sweetie,' a Virtual Girl Created to Target Child Predators' (*CNET*, 5 November 2013) <https://www.cnet.com/news/meet-sweetie-a-virtual-girl-created-to-target-child-predators/> accessed 9 December 2022.

harming children in the process.[66] The Law Commission themselves have recognised that deepfakes can be positive and therefore regulation should only seek to "criminalise the narrow issue of sharing non-consensual altered intimate images."[67] Thus, deepfake technology would not have its development stifled and a view towards responsible innovation could prevent misuse. Von Schomberg defines responsible innovation as a transparent and interactive process, bringing societal actors and innovators together to become mutually responsive in working towards "acceptability, sustainability and societal desirability of the innovation process."[68] With this in mind, it becomes clear why the Law Commission held discussions with various stakeholders, including victim support groups, academics, parliamentarians, and legal professionals.[69] Through these discussions, victims can communicate to lawmakers the harms they have endured, leading to a legislative response that reflects the severity of deepfake pornography.

6. Conclusion

This article has established the severity of deepfake pornography, highlighting how the phenomenon is deeply gendered and violates women's rights. Legislative response through criminal and tort law has failed to adequately capture deepfake pornographic harm. However, various stakeholders should discuss the implications of deepfake pornography and work to update UK law, adapting legislation to address contemporary challenges previously unforeseen. Reforming sections 33 and 35 CJCA based on the Law Commission's recommendations is the first necessary step to prevent AI contributing to IBSA online. Also, through the introduction of the OSB, deepfake pornography can be blacklisted across various platforms and perpetrators consequently found guilty of committing a sexual offence. Furthermore, victims should be enabled to claim against companies who profit from deepfake pornography as doing so clearly undermines their duty of care in their failure to take a stand against IBSA.

---

[66] Claudia Ratner, 'When "Sweetie" Is Not So Sweet: Artificial Intelligence and Its Implications For Child Pornography' (2021) 59(2) *Family Court Review* 386, 396.
[67] Law Commission (n 60), 163.
[68] René von Schomberg, '*Prospects for technology assessment in a framework of responsible research and innovation'* in Marc Dusseldorp and Richard Beecroft (eds), Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methoden (2012th edition, VS Verlag für Sozialwissenschaften).
[69] Law Commission (n 67), 8.

Competition Justice in a Privacy-Anxious Digital Economy

Said Al Hinai

1. Introduction

In recent years, there has been significant growth in the digital economy. Companies can now gather an extraordinary amount of personal data. Moreover, the usage of such data became key to many business models.[1] While big data are increasingly utilized in every aspect of the economy, competition law authorities find themselves questioning the role of big data and related aspects of privacy in competition law.[2] Many critique the EU Commission's approach to handling data and privacy-related issues in the competition law perspective, including Cristina Caffarra,[3] arguing that the Commission should have paid closer attention to privacy reduction when looking into competition issues (mainly merger control and abuse of dominance cases). At the same time, others believe that privacy implications are to be dealt with consumer protection regulation.[4] As Competition Commissioner Vestager pointed out, 'I do not think we need to look to competition enforcement to fix privacy problems. But that doesn't mean I will ignore genuine competition issues just because they have a data link.'[5]

There is much disagreement and uncertainty about the extent to which competition law should consider privacy degradation. The first section of this article will review the developments in privacy-related cases regarding both merger control and abuse of dominance. Then, it will consider whether it is appropriate to fit privacy concerns within a merger investigation. Further, it will address when it is appropriate to consider privacy-related issues under an abuse of dominance with respect to the Bundeskartellamt-Facebook case.

---

[1] Alexander Okuliar and Maureen Ohlhausen, Competition, Consumer Protection and the Right (Approach) to Privacy' (2015)80 Antitrust LJ 121

[2] Massimiliano Kadar and Bogdan Mateusz, '"Big Data" and EU Merger Control - A Case Review' (2017) 8(8) JECL 479

[3] Cristina Caffarra and Johnny Ryan, 'Why Privacy Experts Need a Place at the Antitrust Table' (*ProMarket*, 28 July 2021)<https://promarket.org/2021/07/28/privacy-experts-antitrust-data-harms-digital-platforms/> accessed 14/10/2021

[4] Council Regulation (EC)2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L119, 1-88

[5] Margrethe Vestager, 'Competition in a big data world'(DLD 16, 17 January 2016) <https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big-data-world_en>

2. Merger Control Cases

In 2006, during the Asnef-Equifax case, the Court of Justice set that 'any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the relevant provisions governing data protection.'[6] Later, in the 2008 Google/DoubleClick merger case, the Commission reaffirmed the separation between data protection rules and EU competition law.[7] Thereby, the Commission did not consider the privacy implications of the merged entity. Despite such concerns being acknowledged by Former FTC Commissioner Harbour, she noted the consequents of network effects – fewer search engines, leading to lower incentives for search firms to compete on privacy protections or related non-price dimensions.[8]

In 2014, the Facebook/WhatsApp takeover was another opportunity for the Commission to consider the role of big data and privacy in mergers.[9] In particular, the Commission examined the possible competitive advantage gained from accessing WhatsApp's data, as it used to more strictly adhere to privacy than Facebook.[10] Although such differences raised concerns, Facebook confirmed that it would not change WhatsApp's privacy policy after the merger. Two years later, WhatsApp announced its user data would be shared with the Facebook group of companies.[11] The Commission then concluded that Facebook provided misleading information and slapped a €110 million fine.[12] Although no privacy concerns were looked into during the merger proceedings, the Commission particularly confirmed 'any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.'[13] Nevertheless, some interpreters argue that the tide

[6] (Case C-238/05) Asnef-Equifax v Ausbanc (2006) ECR I-11125 para 63
[7] Miriam Buiten, *Regulating Data Giants: Between Competition Law and Data Protection Law* (Springer 2019) 265
[8] Google/DoubleClick, Statement of Federal Trade Commission (F.T.C. File No. 071-0170, 2007) para 12
[9] Facebook/WhatsApp (Case COMP/M.7217) Commission Decision C (2014)7239 (2014) OJ C417/4
[10] Ibid, para 70–71 and para 102
[11] Ibid
[12] European Commission Press release 'Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover'(*European Commission*, 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369> accessed 14 October 2021
[13] Facebook/WhatsApp (Case COMP/M.7217) Commission Decision C(2014)7239 [2014] OJ C417/4, para 164

has turned and that the Commission no longer set aside concerns over Big Data and privacy.[14] This argument is reflected in the Commission proceedings against the misleading information provided by Facebook, where the privacy impact of mergers was considered.

Similarly, Miller argued that the Microsoft/LinkedIn merger case is another example of such a trend. The Commission imposed conditions intended to permit other competitors to integrate with Microsoft products to maintain an open battleground for creating user-facing features,[15] as it concluded that by combining user databases when incorporating LinkedIn into Microsoft Office, the market position of Microsoft in the operating systems for computers would strengthen the market position of LinkedIn in professional social networks.[16] This could increase LinkedIn's user base, rising the entry barriers and 'tipping' the market in its favour.

Despite this, strictly speaking, LinkedIn's market power concerns network effects rather than privacy itself. Moreover, the Commission noted that privacy could be considered only if viewed as a significant factor of quality by the consumer.[17] Nevertheless, this does not appear to reflect a change in the EU Commission's approach to privacy. Colangelo and Maggiolino stated it doubtlessly depended on privacy rules to protect users' data.[18] Additionally, the Commission confirmed, that the merged entity will be subject to data protection rules, further highlighting that it will be subject to EGDPR.[19]

For the first time, the Commission observed in these last two cases that consumers might see privacy as a significant factor affecting the quality. Therefore, competition may be driven by

[14] Akiva Miller, 'The dawn of the big data monopolists'(2016) 1(1) <https://ssrn.com/abstract=2813004> 7
[15] European Commission Press Release, 'Mergers: Commission approves acquisition of LinkedIn by Microsoft, subject to conditions'(*European Union*, 2016)
<https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4284> accessed 14/10/2021
[16] Microsoft/LinkedIn (Case COMP/M.8124) Commission Decision C(2016) 8404 (2016) OJ C388/4 para 324
[17] Ibid para 350
[18] Giuseppe Colangelo and Mariateresa Maggiolino, 'Data protection in attention markets: protecting privacy through competition?' (2017) 8(6) JECL 363, 365
[19] Microsoft/LinkedIn (n 16) para 177 and 178

less privacy-friendly products and services.[20] However, it neither elaborated nor derived any conclusion from this statement.

3. Abuse of Dominance Cases

In 2016, the Bundeskartellamt investigated Facebook on suspicions of abusing its dominant position and imposing unfair privacy terms on users, stating, 'it is essential to also examine under the aspect of abuse of market power whether the consumers are sufficiently informed about the type and extent of data collected'.[21] Such an approach is seen as a turn away from the Commission's approach.

Interestingly, the same conduct by Facebook was investigated in other Member States (France, Belgium and the Netherlands) for violation of data protection laws by the data protection authorities.[22] More recently, the French Competition Authority refused to hold off Apple implementing privacy changes and the CMA has accepted mere commitments on Google's 'Privacy Sandbox' browser changes concerning the removal of third-party cookies (which is not sufficient as established Facebook/WhatsApp takeover). Arguably sparking a trend, such as Apple's introduction of the "sandbox" and "ATT Private Relay" features, which arguably limit user data access and mask IP addresses, respectively. Thus, giving Apple an unfair advantage over competitors who rely on data collection for targeted advertising which in turn calls for antitrust investigations.

4. Defining Privacy

[20] Facebook/WhatsApp (n 13) para 87 and Microsoft/LinkedIn (n 16), nt 330
[21] Bundeskartellamt, Press Release, 'Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules' (*European Union*, 2016) <https://webgate.ec.europa.eu/multisite/ecn-brief/en/content/bundeskartellamt-initiates-proceeding-against-facebook-suspicion-having-abused-its-market> accessed 14 October 2021
[22] Ibid 15

With the emergence of the digital economy, privacy is not seen as concealing individuals' personal information; instead, literature has started to look into the right balance between protection and disclosure of personal information.[23] A highly relevant definition is Westin's (1967), who defined *privacy* as the individual's ability to control the use of and access to their personal information. From a regulatory perspective, privacy is observed as protecting against the access of personal data and controlling the usage of such data.[24] In this sense, the new GDPR strengthened existing rights and gave individuals control over their data, alongside the e-Privacy Directive.

5. Privacy Within Competition Law

5.1 Merger Control

Theories of harm could emerge from the idea that the digital platforms' market power gained from the network effects decreases incentives to offer high levels of privacy.[25] Moreover, concealed data practices might eliminate privacy-quality competition, since they cannot effectively compare different suppliers to consider which offers better privacy protection.[26] Second, as FTC Commissioner Pamela Jones Harbour stated, the merger of data rich companies will create a new entity with even more tools to profile individuals and invade their privacy.[27] Alongside different theories of harm, the debate on privacy raises the question of which legal path should be followed to reach a regulatory solution. More particularly, the role of both competition law and data protection regulation in addressing data protection concerns must be defined.

[23] Grazia Cecere, Fabrice Le Guel, Matthieu Manant and Nicolas Soulié, *The economics of privacy. The new Palgrave dictionary of economics* (Palgrave Macmillan 2017) 1–11
[24] Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The economics of privacy'(2016) 2(52) JEL 442
[25] Pamela Harbouand TI Koslov, 'Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets' (2010) 76 Antitrust LJ 769, 794
[26] Katharine Kemp, 'Concealed data practices and competition law: why privacy matters' (2020) 16(2) Eur CJ 628
[27] Maurice Stucke and Allen Grunes, *Introduction: Big Data and Competition Policy* (Big Data and Competition Policy, Oxford University Press 2016)

To determine whether competition law is the effective and appropriate tool to address privacy concerns, it is essential to look into the purpose of competition law first. The core goal of competition law is to maximize consumer welfare and target business behaviours that harm it.[28] Nevertheless, non-economic and political goals have a significant role, as Roger Van den Bergh noted. In this context, the central role of the European competition law is market integration.[29] Similarly, the post-Chicago school acknowledge the goals should include consumer choice protection.[30] Concerning merger reviews, the aim is to investigate the impact of a merger on consumers, and the merger is prohibited only if it will substantially threaten competition. Therefore, the central aim is to prevent enhancing market power or facilitating its exercise.[31] Thus, any harm must be merger specific, and the link between the merger and the anticompetitive effects must be close.[32]

Some would argue that EU competition law is concerned with consumer protection. Clearly, privacy relates to such aims and affects consumer welfare; therefore, competition law should be expanded to include privacy and data protection.[33] The recent decision of the European Court of Justice on the abuse of dominance emphasized the importance of preventing practices that cause harm to consumers.[34] In this sense, if the main impact of a merger is to create market power and reduce privacy protection, it may fall on the competition agency to review privacy violations so as to deliver the benefits of competition to consumers.

Another argument emerges from the idea that privacy can be viewed as a non-price competition. Reducing privacy could then be seen as affecting a non-price attribute of

[28] David Balto and Matthew Lane, 'Monopolizing Water in a Tsunami: Finding Sensible Antitrust Rules for Big Data' (2016) 7 <https://ssrn.com/abstract=2753249>
[29] Roger Van den Bergh and Peter Camesasca, 'European Competition Law and Economics: A Comparative Perspective: A Comparitive Perspective'(2nd edn, Sweet & Maxwell 2006) 42
[30] Ibid
[31] Shilpi Bhattacharya and Miriam Buiten, 'Privacy as a Competition Law Concern: Lessons from Facebook/WhatsApp' (2018) 6 <https://ssrn.com/abstract=3785134>
[32] Ibid 7
[33] Christopher Kuner, Fred H Cate, Christopher Millard, Dan Jerker B Svantesson and Orla Lynskey, 'When two worlds collide: The interface between competition law and data protection' (2014) 4(4) IDPL 247
[34] Inge Graef, 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets' (December 7, 2016) 4<https://ssrn.com/abstract=2881969>

competition, which is relevant as competition on price to the competition law.[35] The US merger guidelines confirmed that market power could appear as a form of reduced non-price competition affecting the consumers, such as reduced quality, variety or service, and that privacy protection could be added to this list since it is a significant element of consumer welfare.[36] However, there are many forms of non-price competition that are not considered under competition law, such as efficacy and product safety, instead falling within the scope of other laws. In this view, privacy is considered a standalone concern that is at odds with competition law goals, since it is hard to quantify when compared to output and price.[37] Additionally, consumers have mixed views on the optimum level of privacy. This raises the issue of how to determine when consumer welfare is harmed when a company changes its privacy policy.

In both the US and the EU, competition agency practices and case law suggest that privacy concerns will be addressed if they are liked to lessening competition.[38] Both Sokol and Comerford stated that privacy harm (in itself) is not equal to harm to competition; consequently, data protection or consumer protection should address big data problems.[39] Moreover, competition law should only be heralded when competition is harmed, and it is not concerned mechanics of data collection.[40]

With merger control, some would argue that the merging of data-rich companies and the combination of data in itself gives rice to privacy and data concerns, which jeopardizes competition benefits; but there are several reasons why this might not be true. First, such combination of data creates many efficacies, reflected in improving and providing services for lower costs or even for free, increasing consumer welfare.[41] Second, alerting the traditional competition law to include privacy will result in unequal treatment among mergers depending

[35] Ibid 2
[36] US Department of Justice & Federal Trade Commission, 'Horizontal Merger Guidelines' (2010) 2 <https://www.ftc.gov/sites/default/files/attachments/merger-review/100819hmg.pdf>
[37] Darren Tucker, 'The Proper Role of Privacy in Merger Review' 5 Competition Policy Intl, 2-7
[38] Lisa Kimmel and Janis Kestenbaum, 'What's Up with WhatsApp? A Transatlantic View on Privacy and Merger Enforcement in Digital Markets'(2014) 29(1) ABA 48, 53
[39] Ibid 32
[40] Ibid 32
[41] Andres Lerner, 'The Role of 'Big Data' in Online Platform Competition'(2014) <https://ssrn.com/abstract=2482780>

on subjective determinations of privacy harm.[42] More significantly, it might reduce the incentive for new entities to compete or invent new products. While concerns might arise if a profound pocket market leader acquires a market entrant and innovation or competition is harmed, such mergers to acquire potential competitors will also increase the incentive for start-ups to innovate, and who might be further acquired if they succeed.[43] Besides, the consistent threat of new entrants may force big data companies to invest more in innovation.[44]

Given the potential advantages of the data-rich mergers, privacy concerns from the joined entity and the obtained market power do not automatically require competition law intervention, since no firm has an antitrust obligation to provide the best products quality it can provide. Therefore, firms do not have to provide the best privacy-friendly services available. Instead, if an optimal level of privacy-friendly services is required, other economic regulations should intervene.[45] Moreover, start-ups, such as Snapchat, Tinder, Airbnb and Uber, emerged quickly and displaced data-rich established firms.[46] Indicating, even if data-rich companies wanted to use their dominant position alongside the possessed personal data and manipulate privacy to keep out competitors, they would not be able to do so.

The merger of data-rich companies may raise competition concerns where the market power possessed by the firm might be used to lower its privacy protection. Competition law, in this case, should have a role to play in investigating potential abuses of market power, but such investigation should be restricted within the limits of its current objectives and not as a stand-alone issue. Since the new EU data protection framework has been introduced, there seems to be no reason to exhaust competition authorities with data protection policing.

5.2 Abuse of Dominance

[42] Ibid 2
[43] Olga Batura, 'Challenges of personal data for the competition law analysis' (2016) 18(3) Network Industries Q 3
[44] Ibid
[45] Ibid 19
[46] Ibid 32

The Bundeskartellamt Facebook case will be considered to determine the role of privacy in an abuse of dominance case. As stated above, the Bundeskartellamt decision that Facebook abused its dominant position was based on the argument that the data collection practices were contrary to the data protection law (GDPR), raising the question of the relevance of Facebook GDPR violation to establish abuse of dominants. In contrast with the EU level, where competition law does not directly punish the breach of data protection law,[47] in the VBL-Gegenwert, I and II cases, the German Federal Court of Justice stated that abuse of dominance could rise from a dominant undertaking violating data protection laws.[48]

With the growing importance of the digital market, it is easy to find instances of abuse that are non-price exploitative, such as abusive terms and conditions. Therefore, how broadly or narrowly 'abuse' is to be defined and the scope of competition law must be determined. Generally, the scope is determined by considering whether the firm's market power resulted in the abusive conduct,[49] revealing a causal relationship. There are two different approaches to addressing this issue: a strict one requiring that the conduct was only due or possible to the firm's market power, and a lenient approach that requires only the competition to be negatively affected by the conduct resulting from the market power.[50] For exclusionary abuses, European Courts have interpreted the causality link leniently, stating it is enough that the conduct reinforces the companies dominant position.[51] The Bundeskartellamt for the Facebook case applied the same lenient approach adopted by the European Courts for exclusionary abuses to an exploitative practice case, finding a leeway in VBL Gegenwert cases.[52]

However, it can be argued that it is unwise to take this lenient approach, mainly when it does not concern prices but terms and conditions, since it allows competition authorities to prosecute

[47] Case C-238/05 Asnef-Equifax ECLI:EU:C:2006:734, para 63;Facebook/WhatsApp(Case COMP/M.7217) Commission Decision of 3 October 2014, para 164
[48] Case VBL-Gegenwert I(n 18), para 65 and Case KRR 47/14, VBL-Gegenwert II, decision of 24 January 2017, para 35
[49] Miriam Buiten, 'Exploitative abuses in digital markets: between competition law and data protection law'(2021) 9(2)J Antitrust Enforc 270
[50] Ibid 279
[51] Ibid
[52] Ibid 278

any breach of the law as an abuse of dominance.[53] Exclusionary conduct is only possible if the firm is dominant; without this, it cannot exclude competitors. However, exploitative terms and conditions can be imposed by both dominant and non-dominant companies. This is because most consumers are unaware of the accepted terms and conditions (consumers do not read or understand their lengthy volumes).[54] Firms offering user-friendly do not attract consumers any more than other firms, hence, firms have no incentive to compete.[55] Therefore, regardless of the market power of the company, consumers find themselves at a disadvantage.

This, in turn, shows the importance of the 'causality' between the abuse and the market power to determine the extent of prohibition regarding abuse of dominance.[56] If the strict approach was followed, then it is not abusive for a dominant firm to impose abusive data collection practices. If the lenient approach was taken, conduct independent from the market power would be considered an abuse of dominance. One reason to expand the competition law and follow the lenient approach is to restrain super-dominant platforms with competition law sanctions.[57] But, rather than using competition law to compensate for the shortcomings of other laws, data protection laws should be amended. More importantly, such an approach could take competition law to other jurisdictions; as in the German understanding, any breach of the law could amount to an abuse of dominance since any breach is likely to provide a competitive advantage.[58] This will, in turn, open the door wider to turn competition law as an enforcement tool in other fields of law such as tax, data protection, labour or consumer law.[59]

6. Data Protection and Competition Laws

From an economic point of view, both data protection and competition laws address related but distinct issues. As stated above, competition law protects consumer welfare from harm caused by monopoly power (dominant, merging or colluding firms). For example, a consumer may be harmed for paying too high prices. If the competition is weak in the market, they have no choice

[53] Monopolies Commission, 'Biennial Report XXII: Competition 2018'(1st edn, 2018) para 676
[54] Ibid 50, 282
[55] Ibid
[56] Ibid
[57] Ibid 3
[58] Thomas Höppner, 'Data Exploiting as an Abuse of Dominance: The German Facebook Decision'(2019) 1(1) Lexology1
[59] Ibid

but to accept the price, since the dominant firm has no incentive to offer better prices. Furthermore, if competition becomes more intense, this problem will disappear since firms will be pressured to lower prices or lose customers. Further, data protection laws aim to protect users in situations where there is unequal power in a given transaction, regardless of the firm's market power.[60] Since it aims to protect consumer harm from distinct type of problem: information asymmetries.

As discussed above, although consumers might have access to the terms and conditions of privacy, a lot of time and effort is needed to read them, making the consumers rationally ignorant. Consequently, this type of consumer welfare harm will not be solved by a more competitive market. To tackle the problem of asymmetric information, data protection laws must control the data allowed to be collected and processed to protect consumers. As a result, data protection laws address broader issues than competition law and aim to protect data as a fundamental right as well as the right to privacy.[61]

Some would argue that if competitors can signal their privacy-friendliness policies successfully and compete on them and if consumers show they care about privacy, competition should contribute to less data collection and more privacy protection. However, this proved to be difficult in practice, as both DuckDuckGo and Threema are privacy-friendly, but they achieved only marginal success.[62] Putting aside the limited success reasons, this illustrates that data protection laws and competition law may have distinct but complementary roles in protecting consumer privacy in digital markets. Finally the consent under Art. 6(1)(a) GDPR, and Apple ATT and the "freely given" consent question confirms the link between competition and data protection law, since it concerns highly valuable personal data for online advertising.

7. Conclusion

[60] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law'(2017) 54(5) CMLR1427
[61] Ibid
[62] Ibid

There is no doubt that big data plays a key role in the competition authorities' enforcement priorities. Nevertheless, that does not mean all data-related concerns should be considered by competition law, which is essential for intended purposes and not to solve problems dealt by other fields of law. Competition authorities could step in when privacy is harmed even when dominant firms are complying with data protection rules, to place this extra responsibility. If the harm is independent of the market power then data protection laws may be more appropriate and efficient. This is all to protect the legitimacy of these legal instruments, as if it were used as an 'all-purpose' enforcement tool, it would lose its legitimacy and legal certainty.

As such, new data protection rules, the GDPR, were introduced three years ago in response to the growing importance of data in the digital market. It still does not have the same reputation as competition law, but this will take time. Although the working authorities are bound to overlap, breaches of data protection rules are mainly the responsibility of data protection authorities. Thus, data protection authorities demonstrate the teeth in the era of GDPR and data protection rules. This overlap of data protection and competition requires regulators across Member States to come together and offer a clear regulatory framework of how data protection and competition authorities could collaborate and harmonise to address new issues that the digital market raises. Such a move will ensure clarity and efficacy rather than the two stepping on each other's jurisdiction, as seen in the joint statement between the CMA and the ICO.[63] Finally, ECJ Facebook preliminary ruling will further clarify the relationship between the market power and the GDPR.

[63] CMA and ICO, 'Competition and data protection in digital markets: a joint statement between the CMA and the ICO'(19 May 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf> accessed14/10/2021

What can the DMU Learn from the DMA?

Erin Thomson

Introduction

In recent years the EU and UK have been racing to establish a regime which will be better equipped to deal with the challenges brought about by the digital sector. The digital sector consists of dynamic, fast changing markets dominated by a few key players. Traditional competition law is ex post in nature meaning rules are designed to stop or penalise anticompetitive behaviour after a competition concern has been identified.[1] There have been attempts to apply the ex-post regime in the digital sector which has generated limited success. For example, the recent verdict in the appeal of the Google shopping case confirmed a fine of 2.42(euro) billion was to be imposed by Google and paved the way for many more competition cases in the digital sector.[2] However, ex post competition enforcement involves a long investigative process, followed by in depth analysis of complex issues such as market definitions and dominance and decisions are subject to extensive judicial review.[3] Thus, it is too slow and cumbersome for the digital economy.[4] By the time a decision is reached, these players are already working to further entrench their market power in other areas which can result in more irreversible economic harm.[5] Ex ante regulation is required to proactively prevent future anticompetitive conduct on the market before harm occurs. However, this inevitably involves an element of predicting the next moves of big tech firms which is difficult to say the least.

Recognising the need for ex ante regulation, the EU have introduced the Digital Markets Act (DMA) which aims to ensure fairness and contestability and the UK have proposed the establishment of a Digital Markets Unit (DMU) which will form and enforce a pro-competitive

[1] Madiega, '*Regulating Digital Gatekeepers'*, (European Parliamentary Research Service, 2020)
[2] Google and Alphabet v Commission (Google Shopping) Case T-612/17
[3] Geradin, oral contribution at the 'Strathclyde Centre for Internet Law and Policy Seminar' available at (https://www.youtube.com/watch?v=gzIAyVdSjvE 37:34)
[4] (n 1)
[5] Department for Digital, Culture, Media & Sport and Department for Business, Energy and Industrial Strategy, *'A new pro-competition regime for digital markets'*(GOV UK, 2021) <https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/consultation-document-html-version#part-2-the-digital-markets-unit> accessed 2 November 2021

ex ante regime in the UK with the aim of promoting competition for the benefit of consumers. The DMA came into force on 1 November 2022 and it is hoped the Digital Markets, Competition and Consumer Bill will be introduced in the UK parliamentary session beginning May 2023 which will provide the DMU with some much needed teeth.[6] Despite operating differently, both the UK and EU regime will apply to only the most powerful firms (gatekeepers) and seek to address similar anti-competitive practises. Therefore, it will be sensible for the UK to pay close attention to the operation of the DMA and the academic discussion surrounding it.

1. The regimes

The DMA contains two lists of obligations which gatekeepers must adhere to. The aim is to provide a clear list of 'dos and don'ts'[7] removing the need for lengthy investigations and allowing for quicker enforcement. The focus is on monitoring compliance rather than conducting investigations and assessments. Articles 5 and 6 contain the 18 obligations which are applicable to all designated gatekeepers, hence the DMA is often termed as a one size fits all approach. Article 5 obligations are considered self-executing, meaning all gatekeepers are required to comply within 6 months of designation. The self-executing list has been welcomed as there was a recognised need for straightforward rules which are not open-ended for gatekeepers to interpretate.[8] Article 6 obligations are susceptible to further specification, Article 7(2) prescribes the European Commission to specify the measures a 'gatekeeper' must implement to comply with Article 6 obligations. This allows for a degree of flexibility within the DMA.

Alternatively, the UK regime will take the form of a code of conduct and pro-competitive interventions which are enforceable by the newly established Digital Markets Unit. The code of conduct will be formed around high-level principles, (such as "fair trading, open choices,

[6] HM Treasury 'AUTUMN STATEMENT' (November 2022) <accessed 20 April 2023 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118417/CCS1022065440-001_SECURE_HMT_Autumn_Statement_November_2022_Web_accessible__1_.pdf
[7] Larouche and Streel, '*The European Digital Markets Act: A Revolution Grounded on Traditions'* (2021) 12 Journal of European Competition Law & Practise 542 <https://doi.org/10.1093/jeclap/lpab066>accessed 5 November 2021
[8] ibid

trust and transparency"), set out in legislation and will be capable of being individualised to suit the needs of each SMS firm. Tailoring of the principles would include stakeholder participation and occur during the designation process. [9] The aim of the code is to manage the harmful effects of market power and provide clear guidance to firms with SMS as to their expected behaviour, in turn protecting consumers and businesses.[10] It is hoped clear guidance will enable firms with SMS to adapt their behaviour, preventing anti-competitive behaviour before it occurs. The pro-competitive interventions on the other hand will aim to increase market contestability by addressing the underlying features which allow the firms to reach powerful positions. [11]The DMU will be able to impose specific behaviour and structural remedies on SMS firms where the firm's activity has created an adverse effect on competition.

2. Designation

As both regimes are only applicable to the most powerful firms arguably the most crucial factor within both regimes will be the designation of firms. If regulation is to have any positive impact for competition it is crucial that the rules are applied to the 'real' gatekeepers of the digital markets. The DMA and the proposals from the DMU have taken slightly different approaches to the designation of gatekeeper firms however both regimes will take into account quantitative and qualitative criteria when carrying out the assessment.

The DMA requires firms to self-designate by considering whether their platform provides one of the eight core services listed in Article 2. These include online intermediation services, search engines, social networking video-sharing, interpersonal communication, operating systems, cloud computing and advertising services.[12] Once a firm has qualified as a core platform service provider (CPS), it will be considered a gatekeeper if it satisfies the qualitative criteria. This entails having a significant impact on the internal market, serving as an important gateway for business users to reach end users and enjoying an entrenched and durable position in its operations or such position is foreseeable in the near future.[13] However, crucially, an

[9] (n 5)
[10] Catherine Bathelor oral contribution at the 'Strathclyde Centre for Internet Law and Policy Seminar' available at (https://www.youtube.com/watch?v=PwDBrkmTIkc 25:44)
[11] Ibid
[12] DMA Art.2
[13] DMA Art.3

undertaking will be presumed to have satisfied the qualitative criteria if the quantitative requirements in paragraph 2 of article 3 have been met. Thus, an undertaking is presumed to be a gatekeeper if; the annual turnover of the undertaking to which it belongs is equal to or above EUR 6.5 billion in the last three years or the undertakings average market capitalisation or the equivalent fair market value amounted to at least EUR 65 billion in the last financial year.[14] If upon self-assessment a firm meets the quantitative criteria, it must then notify the commission of its gatekeeper status within 2 months.

The approach is therefore largely mechanistic. As a result, it is largely straightforward and boasts a high degree of certainty which is welcomed by many tech firms. However, reliance on quantitative criteria may contribute to the idea 'big is always bad.' This is detrimental as the largest firms do not always partake in the most harmful conduct and size is not always indicative of status as gatekeeper. For example, *Athney* defines a gatekeeper as "A platform acts as a gatekeeper when it aggregates a *meaningfully large group of participants that are not reachable elsewhere*" [15] with no reference to the size of the platform. Boeston argued the designation thresholds were centred around GAFAM, currently the main service providers.[16] However, this makes sense. It cannot be denied that these are incredibly powerful firms with vast amounts of data and therefore have the biggest potential to impact competition within the digital markets. Swhab highlighted the need to focus on the biggest problems and the biggest bottlenecks first.[17] This is a logical approach.

However, despite this, an awareness of the potential issues which may arise from quantitative criteria remains necessary. Too stringent a focus on quantitative criteria may result in firms slipping through the cracks. For example, firms which come just below the threshold may engage in conduct which the act aims to proscribe without being subject to the rules of the DMA. Whilst other firms who have only just satisfied the threshold will be required to adhere

[14] DMA Art.3
[15] S Athey, "*Platform Markets – Business Models & Gatekeepers*", presentation, November 2020
[16] Boeston, 'Understanding the Digital Markets (2023) 68 The Antitrust Bulletin https://journals.sagepub.com/doi/full/10.1177/0003603X231162998#fn109-0003603X231162998 accessed 5 April 2023
[17] Javier Espinoza, '*EU Should Focus on Top 5 Tech Companies, Says Leading MEP' Financial Times (London, May 31 2021)* https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b <accessed 18 April 2023

to all obligations within the DMA.[18] The solution to this is not found with lowering the threshold as this would simply result in too many undertakings being unnecessarily subjected to the rules of the DMA. Rather, the DMA has attempted to resolve this issue resulting from focus on quantitative criteria by enabling firms to rebut their gatekeeper status and enabling the commission to designate firms even where the quantitative criteria has not been satisfied. However, these two loopholes present a myriad of challenges.

Firstly, the ability of firms to rebut their gatekeeper status may be rather limited. In order to rebut the presumption an undertaking is required to present sufficiently substantiated arguments as to why the firm does not meet the qualitative criteria. Where the commission is satisfied with the argument, a market investigation will be opened. Therefore, the obvious question is, what amounts to a sufficiently substantiated argument? This is unclear. However, it is evident these arguments must meet a high standard of proof.

Article 17(3) states the presumption will only be rebutted in exceptional circumstances and arguments submitted must manifestly call into question the presumption set out in the quantitative criteria of paragraph 2 article 3. Firms seeking to rebut the presumption must meet this high standard all within a 25-page limit which has been set for these sufficiently substantive arguments. Geradin has highlighted the contrast where ex ante regulation of merger control allows for the parties to submit sometimes hundreds of pages.[19] Komninos has also raised doubts as to whether the complex economical and technical assessments required when considering designation are possible based on a 25 page submission. [20] The restrictive page limit appears to be a direct contradiction to the commissions commitment to respecting an undertakings fundamental right to be heard. In addition, Feasey has criticised the inclusion of the term 'exceptionally', arguing it is prejudicial to firms seeking to rebut the presumption and

[18] Andriychuck, '*Shaping the New Modality of the Digital Markets: The Impact of the DSA/DMA Proposals on Inter-Platform Competition*'(2021) 44 World Competition 261 <https://kluwerlawonline.com/journalarticle/World+Competition/44.3/WOCO2021017>accessed 4 November 2021

[19] Geradin '*The draft Implementing Regulation of the Digital Markets Act: Initial thoughts'* (The Platform Law Blog, 2022) https://theplatformlaw.blog/2022/12/12/the-draft-implementing-regulation-on-the-digital-markets-act-initial-thoughts/ <accessed 15 April 2023>

[20] Komninos et al, The Draft DMA Implementing Regulation – Balancing effectiveness with due process?' (White & Case, 2022) https://www.whitecase.com/insight-alert/draft-dma-implementing-regulation-balancing-effectiveness-due-process <accessed 15 April 2023>

is likely t o deter the commission from excluding firms from the DMA.[21] Many firms may meet the quantitative criteria without warranting designation of gatekeeper status therefore should be entitled to rebut the presumption. Evidently, although the ability to rebut the presumption provides a degree of flexibility within the DMA, it will be of limited effect where firms cannot fully utilise this feature within the act.

Secondly, the power of the commission to designate firms irrespective of the quantitative criteria may be too extensive whilst also reducing the certainty of designation within the DMA. In Article 3(5) the commission has specified rebuttal of the gatekeeper presumption will only be possible in exceptional circumstances. However, there is no such specification in relation to the commissions ability to designate firms who do not satisfy the quantitative criteria. Feasey argues the same evidential standard should be applied to all market investigations under article 17.[22] The difference in evidential standard is clear when considering the different lengths of market investigation, Article 17(3) prescribes the market investigation to determine whether a firm should be excluded must be concluded within 5 months. Whereas market investigations to determine whether a firm ought to be included have a time period of 12 months. Feasey notes there is no 'priori reason' why the latter would require more evidence. [23]

On the other hand, it is important not to be overly critical of the designation process within the DMA. The reliance on quantitative criteria does raise some challenges which may not be adequately compensated for however there are benefits to the approach taken. By focusing on quantitative criteria, the DMA 'curbs the shenanigans,' leaving no room for the imagination or for firms to argue against their designation.[24] This helps in the attainment of the aim to speed up enforcement as the DMA is applicable automatically upon qualification. The DMA aims not to follow in the footsteps of ex post competition enforcement and therefore the move away from long winded market investigations should be welcomed as a positive.

---

[21] Feasey, *'NOTE ON DESIGNATION OF GATEKEEPERS IN THE DIGITAL MARKETS ACT'* (Issue Paper, November 2022) https://cerre.eu/wp-content/uploads/2022/11/NoteOnDesignationOfGatekeepersintheDMA_Final.pdf <accessed 21 April 2023>
[22] ibid
[23] ibid
[24] Caffarra, Morton, '*The European Commission Digital Markets Act: A translation'*, (VoxEU & CEPR, 2021) <https://voxeu.org/article/european-commission-digital-markets-act-translation> Accessed 2 November 2021

In the UK a firm will be considered to hold strategic market status where it has substantial entrenched market power in at least one digital activity providing it with a strategic position. This is an evidence based economic assessment conducted by the DMU.[25] A firm is considered to have substantial market power when users lack good alternatives and there is limited threat of entry or expansion by other suppliers. Entrenched market power is established when a firm's market power is expected to persist over time and it is unlikely to be competed away in short or medium term. Where such substantial entrenched market power provides the firm with a strategic position, SMS status is designated.[26] When assessing the presence of a strategic position the DMU take into account the significance of the firm's size or scale in the activity, importance of the firm as an access point to consumers, whether the activity can be used to further entrench or protect market power or extend market power into other activities.[27] In response to the consultation the UK government have since clarified there will be a deadline of 9 months, with the option to extend this by 3 months in exceptional circumstances, for designation assessments. There are significant benefits to the DMUs designation process. The UK government noted, firms with SMS are likely to undertake a range of activities however may only have entrenched market power in some activities. By not applying a general status of SMS to the firm for all activities, focus is placed on the parts of business models which pose the greatest threats to competition and avoids unnecessary burdens on the firms.[28] However, this flexibility also reduces clarity. Respondents to the public consultation on the pro-competition regime highlighted the need for greater certainty as to which firms will come within the scope of the regime. As a result, the government have confirmed they will adopt a minimum threshold to make clear which firms are out with the scope of regulation. This may be a safer approach as opposed to the threshold of the DMA which seeks to target the largest firms rather than simply ensuring the smaller firms are not unnecessarily subjected to the rules.[29]

[25] ibid
[26] (n 5)
[27] (n 5)
[28] (n 5)
[29] GOV.UK '*A new competition regime for digital markets – government response to consultation*' (6 May 2022) <https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/outcome/a-new-pro-competition-regime-for-digital-markets-government-response-to-consultation#part-3-strategic-market-status> accessed 14 April 2023

One aspect of the UKs designation process which requires adjusting is the ability of firms to challenges their SMS status. At present the consultation has suggested firms should be able to dispute their designation where there has been a material change meaning that the SMS status is no longer appropriate. There has been a lack of further clarification on this subject however the DMU should pay close attention to the criticisms of the DMA in this regard. Clear guidance on these rules and the process of disputing SMS status would be beneficial for the regime.[30]

3. Listed obligations v tailored rules

A significant disparity between the DMA and DMU exists in the approach to the rules. Whilst the UK regime is more aligned with the standard rules-based approach which has evolved in competition law, the DMA is closer linked to a per se rules approach. Standard based rules are softer as the legislator determines the standard offering objectives which are used during enforcement. On the other hand, a per se rules approach involves legislators determining rules on prohibited behaviour which are directly enforced.[31] Whilst there are just reasons for adopting a per se rules approach, it is also a main reason why the DMA has been subjected to criticism for being a one size fits all approach.

The DMA approach is often justified on the basis of providing legal certainty. However, failing to recognise the fundamental differences which exist within digital markets and business models has resulted in a 'curious game of charades'[32] as it is unclear how certain obligations will apply to all firms. Evidently, several obligations are directed towards a specific firm. This will make it difficult for other firms to determine how to effectively comply with an obligation which is not directed towards them. Additionally, most obligations can be traced back to previous or ongoing cases, for example, Article 5(3) which prohibits most favoured nation clauses is a reference to the booking.com case, article 6(3) which contends users must be able to deinstall any pre-installed app, stems from the Commission's decision in Google Android

[30] Dunne, '*Pro-competition Regulation in the Digital Economy: The United Kingdom's Digital Markets Unit*'(2022) 67 The Antitrust Bulletin <https://journals.sagepub.com/doi/pdf/10.1177/0003603X221082733> accessed 16 April 2023

[31] Kerber, 'Taming Tech Giants with a Per-Se Rules Approach? The Digital Markets Act from the 'Rules vs. Standard' Perspective' (2021) No.3 Concurrences 28<https://ssrn.com/abstract=3861706 or http://dx.doi.org/10.2139/ssrn.3861706>accessed 4 November 2021

[32] (n 23)

and the prohibition of self-preferencing clearly reflects the google shopping case.[33] Rules derived from cases are generalised to apply to a broad range of platforms thus compounding difficulties when interpreting how obligations apply to a firm and limiting the DMA's ability to adapt to future changes in digital sectors. Uncertainty as to how firms will comply contradicts the rationale behind the DMA and questions the effectiveness of a one size fits all approach.

The UK regime may generate greater certainty as firms will be provided with clear guidance as to how the code of conduct applies to them specifically. Different business models present risks of different competition concerns. For example, ad funded services focus on scaling up users therefore may create difficulties for entrants by establishing defaults to ensure users remain on their platform whereas app stores may make it difficult for developers to operate across other platforms.[34] It is impractical to assume general rules will effectively prevent the multitude of anti-competitive practises which can arise from each platform.

The UK may also be capable of better adapting to future developments as a result of greater flexibility afforded to the regime. Digital markets are fast moving, technology and business models will inevitably change. The UK regime has greater scope to impose obligations in time with technology developments as the DMU are not constrained to a list of obligations. It should be noted the list of obligations in the DMA are not set in stone. Article 10 allows for new obligations to be added to both lists in Article 5 and 6. However, adding obligations would require a market investigation, slowing enforcement. Furthermore, *Kerber* notes, introducing a new obligation would involve analysis on the impact of such obligation on all gatekeepers and may lead to rejection where it is beneficial for only a small number of gatekeepers.[35] Also, it is not sensible to have a long list of obligations which is constantly being added to.[36] The implications of adding to the list could constrain the DMA's ability to adapt to future developments. Facebook has expressed noteworthy doubts on the success of a set list,

[33] Botta, '*Sector Regulation of Digital Platforms in Europe: Uno, Nessuno e Centomila*' (2021) *Journal of European Competition Law & Practice 500* < https://doi.org/10.1093/jeclap/lpab046> accessed 7 November 2021
[34] (n 23)
[35] (n 30)
[36] (n 7)

recognising the difficulty of the Commission to pre-empt the market and future innovation.[37] Several recommendations have been made to increase flexibility within the DMA. For example, increasing flexibility within Art.6 by replacing specific rules with broader principles,[38] presenting the obligations as a menu from which the commission can pick which obligations should be applied to specific gatekeepers or introducing a defence to allow gatekeepers to justify non-compliance with Article 5 in extreme circumstances and Article 6 where pro-competitive effects are possible.[39] Proposals for flexibility are met with fear of reoccurrence of the well-known issues embedded in ex post enforcement. *Geradin* argues the DMA 'should remain targeted to well identified problems.'[40] Undoubtedly, increased flexibility would reduce the impact of automatic applicability. Arguably, the benefit of flexibility in ensuring the DMA is forward looking outweighs the risks of softening the per se rules approach. However, regulation is required now. The DMA will be applicable to firms from May 2023 whilst the DMU has only just began making any progress since 2021. Although it is important for a regime to be future proof, it also requires to be put into action in the first place. There appears to be progress in the UK with the Digital Markets and Competition bill being introduced to parliament at the end of April 2023 however there have been significant changes in the digital markets since the DMU was originally introduced. For example, since the DMU proposal, TikTok has presented a challenge to Facebooks dominance in social media and the integration of ChatGTP into Bing has presented similar challenges to Googles dominance.[41] These changes reflect the quick changing nature of digital market. If the DMU stand any chance of keeping up to date with the digital market's, enforcement is prudent.

4. End users

The focus on end users is one of the main reasons ex ante competition regimes will come under scrutiny. The DMA makes the conscious decision to generalise rules in order to target the most

[37] Facebook, *'Preliminary Comments on the EU Digital Markets Act'* (2021) <https://enterprise.gov.ie/en/Consultations/Consultations-files/Facebook-DMA-Submission.pdf>accessed 13 November 2021
[38] (n 3)
[39] (n 30)
[40] Geradin, '*The DMA should stay true to its principles, or it could fail'*, (The Platform Law Blog, 2021) < https://theplatformlaw.blog/2021/11/08/the-dma-should-stay-true-to-its-principles-or-it-could-fail/> accessed 10 November 2021
[41] Lesh, 'Why the Digital Markets unit poses a fundamental threat to British innovation' (2023, CAPX) <https://capx.co/why-the-digital-markets-unit-poses-a-fundamental-threat-to-british-innovation/> accessed 23 April 2023

harmful conduct which big tech firms frequently engage in. However, this creates an increased risk of errors, particularly type 1 errors where rules prohibit beneficial behaviour.[42] For example, Article 5(3) prohibits gatekeepers from including most favoured nation clauses which prevent business users from offering the same products at different prices or conditions through third-party online intermediation services. This is understandable where such clauses have the effect of dampening competition, for example where prices increase and firms compete less.[43] However, the DMA fails to recognise the beneficial impacts, particularly for consumers, which MFN clauses can bring about. MFNs can increase transparency and reduce search costs for consumers. Consumers may continue to use the gatekeeper website as opposed to third party platform due to the attractiveness of a well-known site and in turn may pay increased prices or receive lower quality services/goods. Incentives for innovation are also reduced as platforms may no longer be able to ensure the best offers. Thus, reducing consumers to endless searching which is often not desirable.[44] Therefore, despite the DMAs objective "to allow end users and business users alike to reap the full benefits of the platform economy and the digital economy at large, in a contestable and fair environment,"[45] the DMA may restrict the benefits offered by gatekeepers. *Geradin* noted the potential for Article 5(2)b to restrict the data free for all by preventing combination of data which is detrimental to consumer welfare and privacy. However, by including the ability to receive consent, the article becomes much less than revolutionary as consumers will continue to be nudged into providing consent.[46]

There is no explicit efficiency defence within the DMA which has led to criticism that the act does not allow for gatekeepers to justify actions on the basis it is beneficial to end users. However, Blockx notes that despite no efficiency defence there is still room for manoeuvre, he argues that recital 23 merely stipulates that efficiency is not relevant for the designation of a

[42] (n 30)
[43] Baker & Chevalier, *'The Competitive Consequences of Most-Favored-Nation Provisions*,' (2013) 27 Antitrust Magazine, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2251165>accessed 13 November 2021
[44] Portuese, *'The Digital Markets Act: European Precautionary Antitrust,'* (ITIF,2021) < https://itif.org/publications/2021/05/24/digital-markets-act-european-precautionary-antitrust> accessed 13 November 2021
[45] European Commission, *'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) Explanatory Memorandum'* (2020) EUR-Lex <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN>accessed 7 November 2021
[46] (n 3)

gatekeeper however there is no such statement about efficiency in regard to article 5-7 of the DMA.[47] This suggests there may be more flexibility within the Act when it is being interpreted.

Tailoring obligations undoubtedly provides for a more flexible regime allowing the DMU to go further when such regulation is warranted whilst also being able to take a step back from regulation when it is not required and could negatively impact efficiency or policy objectives. It is not necessarily the aim to create entirely separate codes of conduct for each firm however individualisation allows regulation to be adapted where practises enhance consumer welfare or innovation.[48] On the other hand, this leaves room for gatekeepers to use their resources to form complex arguments justifying their conduct. Therefore, the DMU must be cautious not to trade off the benefits which come with legal certainty simply to ensure flexibility within the regime.

5. Conclusion

To conclude, it is undisputed that ex ante regulation is required to prevent anti-competitive conduct in the digital economy as ex post enforcement alone is insufficient. The UK and EU regimes aim to target generally similar practises and shortcomings of competition enforcement. However, significant differences exist in the approach of doing so.

Both regimes require to strike a balance between flexibility and legal certainty. The DMA appears to focus on legal certainty which is evident from the reliance of quantitative criteria in relation to the designation of gatekeepers. The DMA does have mechanisms in place to ensure firms can be excluded and included in the regime however further clarification on how this will operate is required. The DMU on the other hand, propose a much more flexible approach with the involvement of in-depth assessments to designate gatekeepers. The minimum threshold is a welcomed development to the DMUs designation process however further clear-cut criteria may be required to ensure harmful gatekeepers can be designated at a pace closer to that of developments in the digital markets.

[47] Blockx '*The Expected Impact of the DMA on the Antitrust Enforcement of Unilateral Practises'* (2023, University of Antwerp) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4341277> accessed 20 April 2023
[48] (n 10)

The DMAs structured obligations may not have the flexibility to adapt alongside new developments and may operate to the detriment of consumers where prohibitions reduce incentives to compete and innovate. By placing greater attention on understanding business strategies and behaviour which may follow, the UK regime is likely more effective in preventing anticompetitive conduct. Prima facie, the UK regime appears to allow for better targeted intervention, which is future proof, specific and seeks to understand the business models of the platforms. However, the DMU may benefit from considering the advantages of legal certainty when it comes to regulating conduct which is harming competition in the digital markets at present.

Apportionment of Cybersecurity Risks in the Private and Public Sectors

Yaxing Shi

1.Introduction

In the past few decades, network technology has become an indispensable part of our daily life, greatly improving productivity, and facilitating people's lives. However, while the network and its related technologies improve people's quality of life, due to the uncertainty of its development, the rapid spread of danger, and the concealment of risks, it also brings a series of risks such as cyber-attacks and cybercrimes. Cybersecurity has become one of the most pressing security challenges of the 21st century.

Compared with other technical fields, the main content of cybersecurity is innovation regulation and risk apportion. And the responsible subjects of cybersecurity risks include individuals, proprietary network service providers, and public sectors. Although the government is an important regulator of cybersecurity, in the market environment, individuals and enterprises, especially network operators and network service providers, have begun to play an increasingly important role in cybersecurity supervision and risk control.

This article discusses the strengths and weaknesses of existing relevant laws by analyzing trends in regulatory regimes that allocate risk between private sector suppliers and government agencies. First, this paper will demonstrate the importance of network security and the evaluation criteria of the network security risk supervision system. Second, I will describe the current EU legal provisions on the allocation of cybersecurity risks. Finally, I will analyze the shortcomings and improvement measure of the existing network security risk allocation system based on the changing trend of the role of proprietary network operators in network security risk allocation.

2.Risk and resilience of cybersecurity

Since the advent of the Internet, almost everything we do in our daily lives has been inseparable from the network system. As the most important tool for the country, enterprises, and

individuals, the Internet plays an irreplaceable role in controlling infrastructure, operating financial markets, and managing personal information. However, as cyberspace occupies an increasingly important position in our lives, cyberattacks have become more frequent and destructive. According to statistics, cyber-attacks cause losses of more than 100 billion U.S. dollars every year. If the potential hazards and indirect effects are considered, the loss may exceed 300 billion US dollars.[1] Therefore, cybersecurity has become one of the most important security challenges in the 21st century.

The definition of cybersecurity is not unique. The main view is that cybersecurity is a collection of methods used to protect cyberspace from cyber-attacks.[2] In terms of purpose, cybersecurity needs to protect the network systems and the information they contain from invasion;[3] reduce the risk of malicious attacks on software, computers, and networks.[4] In content, cybersecurity includes defensive methods for detecting and blocking potential intruders;[5] preventing and organizing cyber-attacks.[6]

Compared with other crimes, cybercrime is cheaper and more convenient. It is not affected by region and distance, and it is difficult to be tracked, so cybercrime is difficult to prevent. It can therefore be expected that the number and sophistication of cyberattacks will continue to grow. As a result, to protect network information and network systems, cybersecurity regulations are necessary to specify the responsibilities of different subjects in the network to deal with various risks in cybersecurity.[7]

---

[1] Julian Jang-Jaccard and Surya Nepal, 'A Survey of Emerging Threats in Cybersecurity' (2014) 80 Journal of Computer and System Sciences 973.
[2] Dan Craigen, Nadia Diakun-Thibault and Randy Purse, 'Defining Cybersecurity' (2014) 4 Technology Innovation Management Review 13.
[3] RA Kemmerer, 'Cybersecurity', *25th International Conference on Software Engineering, 2003. Proceedings.* (2003).
[4] Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (Chatham House 2009).
[5] National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (National Institute of Standards and Technology 2018) NIST CSWP 04162018 <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 1 December 2022.
[6] EM Aupperle, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, vol 52 (American Library Association dba CHOICE 2015) <https://www.proquest.com/docview/1677214011/abstract/B8CBEE95894A43DDPQ/1> accessed 1 December 2022.
[7] Jangirala Srinivas, Ashok Kumar Das and Neeraj Kumar, 'Government Regulations in Cyber Security: Framework, Standards and Recommendations' (2019) 92 Future Generation Computer Systems 178.

Cybersecurity risk refers to the risk of loss due to failure or damage of network systems, including the loss of personal data, the destruction of key facilities, and the occurrence of various cybercrimes. Many market participants currently view cybersecurity risk as one of the most urgent global concerns.[8]

Pervasive and potentially catastrophic threats in cybersecurity have prompted governments and related agencies to develop risk-based standards to protect the cyber domain. However, due to the high degree of uncertainty and rapid change in the cyber field, which is different from other fields, traditional risk assessment measures are less effective in cyberspace,[9] so the concept of resilience has emerged in cybersecurity theory to measure cybersecurity governance.

In the field of cybersecurity, the concept of resilience is often used to evaluate the degree and speed of network system recovery from various adverse events.[10] Resilience refers to the ability to recover quickly to accomplish intended tasks despite a network system being attacked with adverse consequences.[11] Since it is inevitable that network systems are attacked, resilience provides a better way to assess risks in the field of cybersecurity.[12]

3.Evaluation of current law for cybersecurity in the EU

Due to the uncertainty of threats, the rapidity of risk propagation, and the concealment of risks in cybersecurity, the central element of cybersecurity is the regulation of innovation. Considering the uncertainty and high threat of its risks, risk supervision is an important part of it.[13] Since cyberspace is a special domain, it is neither restricted by sovereignty nor national

[8] Chris Florackis and others, 'Cybersecurity Risk' 95.
[9] Zachary A Collier and others, 'Cybersecurity Standards: Managing Risk and Creating Resilience' (2014) 47 Computer 70.
[10] Andre Barrinha, 'Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy' (2016) 25 European Security 387.
[11] Alvaro Rocha and others (eds), *New Contributions in Information Systems and Technologies: Volume 1*, vol 353 (Springer International Publishing 2015) 327.
[12] Igor Linkov and José Manuel Palma-Oliveira, 'An Introduction to Resilience for Critical Infrastructures' in Igor Linkov and José Manuel Palma-Oliveira (eds), *Resilience and Risk* (Springer Netherlands 2017).
[13] Janine S Hiller and Roberta S Russell, 'The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison' (2013) 29 Computer Law & Security Review 236.

boundaries, and individual activities are difficult to track and control, which makes it extremely difficult for any individual or group to carry out independent risk supervision. On the one hand, the public sector needs to play a role in risk prevention; on the other hand, the private sector needs to promote market vitality and information flow while providing secure network services. Therefore, it is necessary to manage it by cooperating with a series of public departments and private sectors.[14]

At present, allocation of responsibility for risks to different groups in the EU is preliminarily established by various regulatory systems. Directive 2016/11481 on security of network and information systems (the NIS Directive) is the first legislation undertaken at the European Union (EU) level for the protection of network and information systems across the Union, which mainly stipulates the allocation of risk responsibilities between the public the private sector. The NIS directive aims to improve the level of resilience of critical data in network infrastructure.[15] The Directive introduces obligations such as incident reporting for the private sector, including essential service operators and digital service providers, while further imposing responsibilities on member states.[16]

The main significance of the NIS Directive is to prevent and reduce the impact of network attacks by managing network risks and notifying cybersecurity incidents, thereby improving the resilience level of critical infrastructure to cybersecurity.[17] NIS Directive consists of 27 instructions. Articles 1 to 6 set out its scope of effect, the definition of the subject, and the definition of risk. Articles 7 to 10 describe the obligations of the state and the government-led public sector to introduce national strategies, create cooperative groups, and oversee critical industry cybersecurity. Articles 14 to 20 set out the obligations of the private sector, essential

[14] Milton L Mueller, 'Against Sovereignty in Cyberspace' (2020) 22 International Studies Review 779.
[15] Alessandro Mantelero and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2020) 28 International Journal of Law and Information Technology 297.
[16] Helena Carrapico and Andre Barrinha, 'European Union Cyber Security as an Emerging Research and Policy Field' (2018) 19 European Politics and Society 299.
[17] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review.

service operators, and digital service providers in Article 4, to provide secure services and event notifications.[18]

The NIS Directive stipulates that the private sectors have the obligation to deal with adverse events and notify relevant official departments when responding to cybersecurity risks, but it is limited to key industries and infrastructure represented by electricity. For the public sector, the NIS Directive stipulates the obligation to build a national framework and national strategy, which is to complete cross-border cooperation and mutual communication among EU member states and to respond and recover in a timely manner from adverse events in cybersecurity.[19]

Although the NIS Directive has given the private sector, represented by network operators, the regulation rights and risk response capabilities of cybersecurity to a certain extent, compared with the current dominance of the private sector in cyberspace, the degree of freedom and power is still limited. The NIS Directive has led to major changes in the cybersecurity regulatory measures in many EU countries. However, with the digitalization of the internal market and the digital transformation of society, cybersecurity risks are constantly evolving, new challenges are emerging, and the NIS Directive has been difficult to adapt to current needs.[20] Investigation shows that the NIS Directive does not cover and regulate all private sectors that provide critical network services. In addition, NIS Directive was deemed to give EU member states too broad a discretion to enforce necessary cybersecurity and incident reporting requirements, while the NIS Directive was deemed incapable of effective surveillance and enforcement.[21]

[18] Rhona Smith, 'Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010' in Rhona Smith, *Core EU Legislation* (Macmillan Education UK 2015) <http://link.springer.com/10.1007/978-1-137-54482-7_33> accessed 4 December 2022.
[19] Alan Calder, *Network and Information Systems (NIS) Regulations - A Pocket Guide for Operators of Essential Services* (IT Governance Publishing 2018) 21 <http://www.jstor.org/stable/j.ctv62hgg9> accessed 4 December 2022.
[20] Sandra Schmitz-Berndt, 'Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way Reports: European Union' (2021) 7 European Data Protection Law Review (EDPL) 580.
[21] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 2020.

4.Trend and improvement of current cybersecurity risk apportion

The way to assign regulatory responsibility for cybersecurity is important because the regulation of innovation is a complex process, and the regulatory regime may hinder technological innovation and development if the relevant rules restrict certain activities that the private sector can reasonably carry out.[22]The disadvantage of the NIS Directive is its limited scope, as the directive applies only to providers of certain digital services and operators of essential services, limited to energy, transport, banking, financial market infrastructure, the health sector, drinking water supply, and distribution and digital infrastructure. Because of this limitation, NIS Directive failed to address the increasing interconnectedness and interdependence among sectors not covered. This could lead to companies underinvesting in cybersecurity as they are outside the scope of the directive.[23]

Explanatory Memorandum to the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 showed that the implementation of the NIS Directives proved to be unsatisfactory in terms of depth and level of coordination. The deficit in national implementation of NIS Directives has resulted in the overall level of cyber resilience in the critical infrastructure sector remaining low.[24]

Network governance capitalism argues that the private sector is increasingly becoming one of the players in network governance.[25] Therefore, there are theories that, in the risk regulation of cybersecurity, the private sector can not only be the provider of cyber services, but also the protector of cyber resilience and the shaper of cybersecurity management policies.[26] A significant proportion of infrastructure and service providers are under the control of the private

[22] David Thaw, 'The Efficacy of Cybersecurity Regulation' (2013) 30 Georgia State University Law Review 287.
[23] CEPS and others, *Study to Support the Review of Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (NIS Directive), No. 2020-665: Final Study Report* (Publications Office of the European Union 2021) <https://data.europa.eu/doi/10.2759/184749> accessed 3 December 2022.
[24] 'EUR-Lex - 52020PC0823 - EN - EUR-Lex' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020PC0823> accessed 3 December 2022.
[25] Eviatar Matania, Lior Yoffe and Tal Goldstein, 'Structuring the National Cyber Defence: In Evolution towards a Central Cyber Authority' (2017) 2 Journal of Cyber Policy 16.
[26] Helena Carrapico and Benjamin Farrand, '"Dialogue, Partnership and Empowerment for Network and Information Security": The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers' (2017) 67 Crime, Law and Social Change 245.

sector.[27] Private companies are the major owners of data and digital infrastructure. The responsibilities of the private sector in cybersecurity regulation typically include acting as a driver of innovation to enhance technological and economic development; complying with relevant laws to maintain order; acting as a guarantor of cybersecurity to create a safer cyberenvironment and Protect citizen data from foreign interference, etc.[28] Therefore, compared with the government, the private sector, as an expert in cybersecurity, has a better understanding of how to regulate the network field.[29] Compared with the government sector, the private sector is more efficient, more stable, and apolitical, so it can often play a better role in the supervision of cybersecurity.[30]

To deal with cyber-attacks on a wider range of industries, on November 10, 2022, the European Parliament approved a directive on common high-level cybersecurity measures across the EU ("NIS2 Directive"), which aims to further development of the legislative framework and levels of security. The purpose of the NIS2 directive is to overcome the deficiencies of the existing directives and provide a more general regulation, allowing the application of specific departmental regulations on cybersecurity risk management measures and incident reporting.[31] NIS2 Directive expands companies covered and their obligations, which is beneficial to improving the overall level of cyber resilience.[32]

5.Conclusion

In conclusion, as one of the most basic topics in cybersecurity, risk apportion is mainly targeted at the public and private sectors. With the rapid development of network technology and the increasing demand for market liberalization, private network service operators, as the main

[27] David Harvey, 'Neo-liberalism as Creative Destruction' (2006) 88 Geografiska Annaler: Series B, Human Geography 145.
[28] 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust' (*European Commission - European Commission*) <https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 3 December 2022.
[29] Myriam Dunn Cavelty and Florian J Egloff, 'The Politics of Cybersecurity: Balancing Different Roles of the State' (2019) 15 St Antony's International Review 37.
[30] Benjamin Farrand and Helena Carrapico, 'Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity' (2022) 31 European Security 435.
[31] Andreas Gruber and Natalie Ségur-Cabanac, 'Necessary or Premature? The NIS 2 Directive from the Perspective of the Telecommunications Sector' (2021) 2 International Cybersecurity Law Review 233.
[32] Thomas Sievers, 'Proposal for a NIS Directive 2.0: Companies Covered by the Extended Scope of Application and Their Obligations' (2021) 2 International Cybersecurity Law Review 223.

owners and providers of network technology, are gradually changing their role from being regulated to policymakers in cybersecurity.

In this process, the NIS Directive played a significant role as the EU's first cybersecurity act, stipulating the risk apportion and regulatory obligations of the private sector in key industries and infrastructure, but the scope of power and risk responsibilities of the private sector Insufficient allocations make it hard to meet the objective of providing cyber resilience to achieve cybersecurity of the EU relations infrastructure.

The NIS2 directive, as a perfection and supplement to the existing laws, is expected to provide a fairer network environment for the entire EU, but the effect of the implementation needs further observation and analysis.

Wearable devices versus wearable medical devices and their regulatory challenges and proposals

Sharon Rose Sooriyakumar

1. Introduction

A new technology that has been on the rise since it was released to the public is wearable devices (WD).[1] A study in 2014 predicted that "more than 30 percent of consumers plan to purchase a wearable fitness device in the next five years."[2] WD are devices that are worn by human, which collects data and keeps track of a person's daily activities like exercise, eating habits, sleep patterns and their weight.[3] Examples of WDs include smart watches, smart cameras and fitness trackers.[4] In the medical field, WD consist of wearable fitness devices, insulin monitors, ECG monitors and wearable blood-pressure monitors.[5] This paper will argue that WD in general are not legally safe however WD in the medical field may be Justified. This paper will be focusing on WD especially in the medical field and will identify its social, economic, ethical, and cultural effects in the wider world. This paper will also analyse the regulatory challenges these effects present and then will propose what the most appropriate regulatory response is.

2. Different types of benefits of wearable medical devices

The medical and social benefits of wearable fitness devices in the wider world are that the problem of medical errors can be solved using these wearable medical devices (WMDs) as health care providers can supply more effective, personalised treatment for the patients that use such devices.[6] This device was effective for when patients had telephone consultations with their doctors during the pandemic as they did not have to go to the hospital in person, for

[1] Steven Spann, 'Wearable Fitness Devices: Personal Health Data Privacy in Washington State' (2016) 39 Seattle U L Rev 1411
[2] ibid
[3] Angela Foster, 'Legal Implications of Data from Wearable Devices' (2016) 42 Litig News 26
[4] ibid
[5] ibid (n 1), 1415
[6] Steven Spann, 'Wearable Fitness Devices: Personal Health Data Privacy in Washington State' (2016) 39 Seattle U L Rev 1411,1415

example to monitor their blood sugar levels.[7] This could lead to other medical innovations in the future.[8] They can also do medical tests from their own home, which the doctors can assess online.[9] An economic effect of WMDs is the fact that it may "dramatically, alter the current healthcare economics landscape."[10] WMDs will save forty billion a year in healthcare costs due to digital and home health visits.[11] In addition, the ethical effect of WMDs is that patients may hold this device accountable when managing their health, which in return leads to better health outcomes.[12] However, some companies make it clear that medical devices are not intended to be used as a source that provides expert medical information and they must be disregarded in favour of specialist medical advice. A cultural effect of WMDs is that as with all technologies, countries that are reluctant to adapt to technology in general will have a challenging time trying to accept these devices into their country and make use of it.[13] Some countries lack knowledge on use of technologies as well.[14]

3. Risks of WDs and WMDs

The stakeholders for medical devices are the public, scientists, health care, doctors, and patients. The risks and hazards of WD in general consists of cyber risks, bodily injury risks to the consumer, technical faults and omission risks for the manufacturers of these products.[15] The manufacturer must ensure that data protection is in place to address customers safeguarding concerns.[16] They must also try to mitigate the risk of product liability claims by

[7] Jacob Hauschild, 'Social Distancing with Your Doctor: The Promise of Telemedicine in Medicare and Medicaid, and How to Pay for It' (2021) 22 Minn JL Sci & Tech 117,124.
[8] Adam D. Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation' (2014) 21 Rich JL & Tech 1, 23.
[9] ibid
[10] Jessilyn Dunn, Ryan Runge, Michael Snyder 'Wearables and the medical revolution' [2018], 429-448.
[11] ibid
[12] Andria Bianchi, 'What to wear? The ethical benefits and challenges of wearable devices' (Hospital news) < https://hospitalnews.com/what-to-wear-the-ethical-benefits-and-challenges-of-wearable-devices/#:~:text=Wearable%20devices%20may%20help%20people,to%20positive%20health%2Drelated%20outcomes. > 10 February 2023.
[13] Yang Meier D, Barthelmess P, Sun W, Liberatore F Wearable Technology Acceptance in Health Care Based on National Culture Differences: Cross-Country Analysis Between Chinese and Swiss Consumers J Med Internet Res [2020].
[14] ibid
[15] Travelers Risk Control, 'How companies can reduce risk from wearables' (Travelers) < https://www.travelers.com/resources/business-industries/technology/how-companies-can-help-reduce-risk-from-wearables > 10 February 2023.
[16] ibid

conducting extensive tests.[17] Manufacturers must avoid technological errors by placing disclaimers to avoid economic loss caused by these technical errors[18]. However, some may argue that these exemption clauses in terms of liability may be in place as a general limitation of liability clauses and not because the devices are unsafe.[19] The above indicates that due to the many risks of WD, they may not be safe, however WMDs use can be justified due to their many benefits listed above. Also, WMDs benefits ensures procedural legitimacy as for the utilitarianists, this device's benefits will give the greatest good for the greatest amount of people (net utility).[20] Similarly, WMDs risks are of cybersecurity concerns, access to personal data and vulnerability to hacking.[21] Kaspersky has found thirty-three vulnerabilities in the data transfer protocol for WMDs.[22] The pandemic has led to the breach of patients' data.[23] An extremely dangerous hazard of WMDs is that a healthcare provider may misdiagnose a patient based on insufficient or inaccurate data.[24] However, some doctors may use the data from medical devices such as an ECG to investigate an underlying problem rather than to make an actual diagnosis.[25] Also, WMDs may challenge the health and safety regulations already in place by the US food and drug administration (FDA) and other governmental agencies.[26]

A recent risk for users of medical devices is that they may die or get severely ill if they catch the deadly fungal infection that is currently, rapidly spreading in the US.[27] This is a new risk and something that the inventors could not have anticipated when making these life saving devices.[28] Situations like this showcase how pandemics create an unanticipated emergency for regulations.[29]

---

[17] ibid
[18] ibid
[19] ibid
[20] Roger Brownsword and Morag Goodwin, '*Law and the technologies of the twenty-first century: text and materials* (CUP 2012) 46-71.
[21] Tyrone Jackson, 'Wearable healthcare devices put patients at risk' (BairesDev Blog) < https://www.bairesdev.com/blog/wearable-healthcare-devices-patients-risk/ > 12 February 2023.
[22] ibid
[23] ibid
[24] ibid
[25] https://www.betterhealth.vic.gov.au/health/conditionsandtreatments/ecg-test
[26] Tyrone Jackson, 'Wearable healthcare devices put patients at risk' (BairesDev Blog) < https://www.bairesdev.com/blog/wearable-healthcare-devices-patients-risk/ > 12 February 2023.
[27] BBC News, 'Candida auris fungal infections spreading in US at 'alarming' rate, says CDC' (BBC News, *23 March 2023*) < https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom/outcome/chapter-4-registration-and-udi > 24 March 2023.
[28] Ann Blandford and Dominic Furniss and Chris Vincent, 'Patient safety and interactive medical devices: realigning work as imagined, and work as done' [2014], 107-110.
[29] ibid

4. Current regulations of WMDs and their regulatory challenges

The relevant regulations of WMDs are the medicines and healthcare products regulatory agency (MHRA) in the UK.[30] In the USA, US food and drug administration (FDA) is regulating medical devices, and they try to reduce the risks of cybersecurity.[31] The US Federal Trade Commission (FTC) is involved in promoting WMDs safety as well.[32] Regulators like the FTC have assessed these risks by publishing a policy statement, which requires consumers to be notified when their health data has been breached, (the health breach notification rule).[33] There is a clash between the precautionary principle and permissionless innovation in the world of WMDs as the precautionary principle prevents new innovations from being allowed if they do not meet current laws, norms, and traditions.[34] Whereas the permissionless innovation allows innovations to be permitted by default and deals with any problems that may develop later.[35] Regulators, regulatory activists, and policy makers are arguing for a policy action on any privacy or security related concerns.[36] Peppett suggests that innovation should be curtailed or tightly regulated to prevent such harm or concerns from developing, this is linked to the precautionary principle.[37] A criticism surrounding medical device regulations in the United States is that a recent analysis has revealed an increase in the number of medical devices recalls.[38] Also, there is a surge in the number of manufacturer field safety notices in the UK over the past few decades.[39] These situations reflect an extremely low standard that is currently used to gain regulatory approval in the wider world.[40]

---

[30] Medicines and Healthcare Products Regulatory Agency (MHRA), 'Medical devices regulation and safety: detailed information' (Gov.UK 2023) <https://www.gov.uk/topic/medicines-medical-devices-blood/medical-devices-regulation-safety> 10 March 2023.
[31] Food and Drug Administration (FDA) 1995
[32] Federal Trade Commission (FTC) (USA), 'Federal Trade commission' (2023) <https://www.ftc.gov/>15 March 2023
[33] Federal Trade Commission (FTC) (USA), 'Medical Equipment and Devices' (2023) < https://www.ftc.gov/industry/health-care/medical-equipment-devices> 10 March 2023.
[34] Adam D. Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation' (2014) 21 Rich JL & Tech 1, 38
[35] ibid
[36] ibid
[37] ibid, 40
[38] May Lee, 'Artificial Intelligence/Machine Learning-Based Medical Devices: Regulatory and Patentability Challenges' (2021) 10 Penn St JL & Int'l Aff 232,261.
[39] ibid 262
[40] ibid

On the other hand, Europe take a different approach when regulating WMDs, originally, they used to follow directives and require manufacturers to ensure their device complies with the essential requirements illustrated in the directive.[41] The essential requirements are the medical devices do not endanger the medical condition or the patient's safety and must not affect the health of the user.[42] However, recently they reformed their regulatory framework with the medical devices' regulation MDR.[43] This regulation contrasts with the directives as they considered that directives made in the 1990s will not be suitable for new technologies such as WMDs.[44] This reform has improved transparency because they make information relating to medical devices available to the public.[45] The 2017 Europe regulation which has amended the directive 2001/83/EC[46], has acknowledged the need for a "robust, predictable and sustainable regulatory framework" for medical devices to ensure the highest level of safety as well as supporting innovation.[47] In Europe private companies regulate device approvals, whereas in the US the FDA regulate medical devices for commercial purposes.[48] Additionally, Health insurance providers around the world are starting to experiment with wearables, which will likely drive greater regulatory interests.[49]

Medical devices have many issues that are not noticed by the appropriate agencies.[50] In the US and Europe, there are restricted abilities to trace most medical devices, hence when problems or recalls transpire, it becomes impractical to understand the extent of the problems without suitable traceability.[51] Patient data privacy and security are additional requirements, which will contribute to the susceptibilities of the present regulatory framework.[52] This is because the

[41] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.
[42] ibid
[43] Regulation (EU) 2017/745- Medical Devices Guidelines
[44] ibid
[45] ibid
[46] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use.
[47] May Lee, 'Artificial Intelligence/Machine Learning-Based Medical Devices: Regulatory and Patentability Challenges' (2021) 10 Penn St JL & Int'l Aff 232,261.
[48] ibid
[49] ibid
[50] May Lee, 'Artificial Intelligence/Machine Learning-Based Medical Devices: Regulatory and Patentability Challenges' (2021) 10 Penn St JL & Int'l Aff 232, 262.
[51] Ibid 263
[52] ibid

necessary requirements to ensure efficacy and safety are yet to be established.[53] Furthermore, in recent years, the public's demand for information about devices and the regulatory process to be "accessible and transparent" has increased.[54] This implies that US and Europe must take immediate action to improve the exchange of information.[55] It has been argued that these issues can be settled with "a more robust medical device regulation system that is harmonised between countries."[56]

5. Regulatory proposals for WMDs

A regulatory response to WMDs is that legislators should pass certain laws that "afford increased regulatory control over data collection."[57] Although, some portion of the data taken from WMDs is beneficial to the users of the device, they are also high value business interests that will keep increasing.[58] Therefore, the advantages of WMDs should be balanced against the infringement of privacy because when privacy is lost, it can never be regained.[59] This strongly, highlights the need for increased regulation even if it may lead to reduced access to data and reduced business profits.[60] Many will argue that privacy needs to be protected in the long-term as it is "a socially and personally valuable commodity", that must be protected at all costs.[61] In Marx's list to safeguard, data protection and security is included.[62] The US and Europe can begin with incorporating the UK's secure data environment platform, where researchers can still access medical information without being restricted as this platform does not allow unverified users to access the data.[63] This regulatory response does not prevent future innovations of medical devices either.

---

[53] ibid
[54] ibid
[55] ibid
[56] ibid
[57] Steven Spann, 'Wearable Fitness Devices: Personal Health Data Privacy in Washington State' (2016) 39 Seattle U L Rev 1411, 1432.
[58] ibid
[59] ibid
[60] Steven Spann, 'Wearable Fitness Devices: Personal Health Data Privacy in Washington State' (2016) 39 Seattle U L Rev 1411, 1432.
[61] ibid
[62] Roger Brownsword and Morag Goodwin, '*Law and the technologies of the twenty-first century: text and materials* (CUP 2012) 46-71, 69.
[63] Department of health and social care, 'Secure data environment for NHS health and social care data-policy guidelines', 23 December 2022 <https://www.gov.uk/government/publications/secure-data-environment-policy-guidelines/secure-data-environment-for-nhs-health-and-social-care-data-policy-guidelines>, 10 March 2023.

It has been argued that understanding the core differences between US and EU medical regulations is vital when developing a new regulatory framework.[64] This provides an opportunity for regulators to amend existing gaps while developing an effective regulatory framework for the future medical devices.[65] Due to the political pressure to significantly repair the existing regulatory framework, this could be the "first step to creating a globally harmonised medical device regulation system."[66] Regulators state harmonised regulations are needed because they reduce redundant reviews, create the opportunity to share information on product safety, and result in a more efficient regulatory regime.[67] The net results will make way for improved trade in medical devices and safer products for the public.[68] Hence, one can argue that a new regulatory framework for medical devices can be created by merging the US and Europe's regulations together after fully understanding their current major differences.

Another proposed regulatory response for WMDs and any other medical devices is from the UK, this will be the most appropriate regulatory proposal as it takes into consideration the implications of the (covid-19) pandemic.[69] The UK's departure from the European union has given them the opportunity to make a UK specific regulatory system, where "patients are at the heart of the decision-making processes."[70] They are planning to increase patient representation on expert groups for medical devices and research advice.[71] They plan to provide simple evaluations of medical devices that are easier to understand.[72] The UK propose to respond more quickly to new advances in technology and work with other "like-minded" international

[64] May Lee, 'Artificial Intelligence/Machine Learning-Based Medical Devices: Regulatory and Patentability Challenges' (2021) 10 Penn St JL & Int'l Aff 232, 261.
[65] ibid
[66] ibid
[67] May Lee, 'Artificial Intelligence/Machine Learning-Based Medical Devices: Regulatory and Patentability Challenges' (2021) 10 Penn St JL & Int'l Aff 232, 261.
[68] ibid
[69] Department for business, energy, and industrial strategy, 'New Proposals to strengthen medical devices regulation and bolster UK life science sectors,' 19 August 2021 <https://www.gov.uk/government/news/new-proposals-to-strengthen-medical-devices-regulation-and-bolster-uk-life-sciences-sector>, 11 March 2023.
[70] ibid
[71] ibid
[72] Medicines and health care regulatory agency (MHRA)-Consultation chapter 4- Registration and UDI', (consultation of future regulators of medical devices in UK), 26 June 2022 < https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom/outcome/chapter-4-registration-and-udi>, 12 March 2023.=

countries.[73] Due to the pandemic disruptions, the UK are now trying to address the delays in medical device approvals, to effectively authorise equipment quicker.[74] The Medicines and Medical Devices Act 2021 (MMDA)[75], allows the maintenance of the regulatory system to support UK's innovation and protect patients' safety as well.[76]

6. My proposition

In my opinion, the regulation of health care devices should be relaxed as their benefits outweighs their risks. Health is important because in article 35 of the EU charter of fundamental rights[77], everyone has a right to benefit from medical treatment.[78] WMDs acts as an aid in achieving suitable medical treatments.[79]Although, this no longer applies in the UK, health is important for all countries regardless. The relaxation of the regulation can be done by removing the precautionary principle. The reason for my suggestion being that mobile phones present a risk to human health, yet many still use them.[80] Therefore, why should medical devices like WMDs and pacemakers be strictly regulated, when they have many health benefits. Also, the precautionary principle reduces and compromises autonomy and intelligence.[81] As Sunstein clearly states, the precautionary principle fails to take into consideration the benefits of such devices.[82] Medical devices are used to benefit peoples' health in the long term, and unlike the technology of brain imaging, these devices will not be used in court rooms to assess credibility.[83] According to Marx's list if the technology is a threat to human health, then prudential consideration is crucial, however if it is not risky then "prudential cases have a lower

[73] May Lee, 'Artificial Intelligence/Machine Learning-Based Medical Devices: Regulatory and Patentability Challenges' (2021) 10 Penn St JL & Int'l Aff 232, 261.
[74] ibid
[75] Medicines and Medical Devices Act 2021
[76] ibid
[77] EU charter of fundamental rights, Article 35- Health Care
[78] ibid
[79] ibid
[80] Roger Brownsword and Morag Goodwin*, 'Law and the technologies of the twenty-first century: text and materials* (CUP 2012) 46-71, 47.
[81] ibid
[82] ibid
[83] ibid

profile."[84] WMDs may not seem to be significantly risky and therefore the regulation can be relaxed to a certain extent.

7 Conclusion

Overall, the above arguments imply that WMDs may be difficult to license, however with the new proposed regulatory response, they can be legally safe to use. We can only justify the usage of WMDs due to their medical benefits, however other WDs such as smart watches may not be necessary as they have more hazards than benefits. The unnecessary devices are the ones with no sufficient medical benefits. WMDs have so many medical and economic benefits, thus they need to be regulated in a way that they are legally safe to use and where the issue of privacy concern is fully addressed. Although WMDs pose some risks as with any devices, these can be sorted out with effective regulatory responses like the one proposed by the UK's report.[85] The best proposal for all medical devices will be the one proposed by the UK in their 2021 report[86] as this takes into consideration the pandemic and prioritises patient's safety. Hacking is a major risk for WMDs, this can be regulated by developing on the current secure data platforms in place in the UK. A note for future researchers is that the regulation of medical devices can be relaxed by removing the precautionary principle as the precautionary principle hinders innovation. The benefits of these medical devices outweigh the risks. If the regulation of medical devices was made stricter, the many patients with medical conditions in need of a medical device will suffer as inventors may stop creating such devices or will be reluctant to create similar devices in the future. To conclude, now WMDs may not be completely, legally safe to use, however with effective regulatory responses according to effective proposals, this can be easily resolved to ensure they are legally safe for consumers to use and manufacturers to sell.

---

[84] Roger Brownsword and Morag Goodwin, *'Law and the technologies of the twenty-first century: text and materials* (CUP 2012) 46-71, 69.

[85] Department for business, energy, and industrial strategy, 'New Proposals to strengthen medical devices regulation and bolster UK life science sectors,' 19 August 2021 <https://www.gov.uk/government/news/new-proposals-to-strengthen-medical-devices-regulation-and-bolster-uk-life-sciences-sector>, 11 March 2023.

[86] ibid

The other side of the coin: privacy justifications in anticompetitive proceedings under Article 102 TFEU

Arletta Gorecka

1. Introduction

With the rise of Web 2.0, and a variety of other digital services and products, personal data represents a key input to a growing number of digital services and products, including, but not limiting to, social networks, search engines, and/or online dating services. Data could be harvested by digital platforms across different devices, such as computers, laptops, and tablets. The ability to acquire and process unlimited quantities of personal data has become a source of competitive advantage, raising antitrust issues and potential breaches of data privacy. However, as the competition authorities are gradually considering privacy in competition law assessments, treating them as an element of abuse of dominant position, this article turns to discuss to what extent undertakings could rely on improvements of privacy to avoid anticompetitive liability, within Article 102 TFEU. This is one of the most nascent interactions on the horizon between competition law and data privacy law. This article assesses efficiency and objective justifications under Article 102 TFEU to assess whether the increased protection for an individual's data privacy could justify otherwise anticompetitive conduct. To scrutinise the findings, the recent developments introduced by Google and Apple are discussed in relation to their possible efficiency and objective justifications.

2. Competition-privacy puzzle: overview

The distinction between data protection and competition law has become unclear with the rise of the GAFAM firms. The early contribution has suggested that the collection of personal data and privacy effects are important to be considered in the competition law.[1] The dominant view remains that competition law should protect competition, while concerns relating to data

[1] Case B6-22/16 *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*. <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108> Accessed 28 August 2019; the German Federal Court of Justice case (2020): Case KVR 69/19, *Facebook v Bundeskartellamt* <https://www.bundesgerichtshof.de/SharedDocs/Termine/DE/Termine/KVR69-19.html;jsessionid=F09CB5804920B1DDFF6B994C11C0E3D8.2_cid286?nn=11439166> accessed 30 June 2020.

privacy should be addressed by data protection or consumer law.[2] In summary, digital change and the expansion of businesses present issues for both legal systems, and it is still unclear how much competition law and privacy interact.

Fundamental issues and similar corrective measures are shared by data protection and competition policies: how to lessen unfairness by putting and enforcing responsibilities on individuals who possess information or market power. The objective is to stop the imbalance of power between powerful people and powerful corporations. The exploitation of personal data is, however, only partially addressed by data protection regulations. The long-term disadvantages to platform users, as well as the special responsibilities that could maintain some digital platforms' dominant positions, are not recognised by data privacy regulation. Thus, to what extent could privacy-related harms be rectified by competition law?

The literature acknowledges two different points of view on how privacy and competition law interact.[3] According to the first theory, competition law is not relevant to data protection law. *Asnef-Equifax* case, where the court disregarded the connection between competition law and privacy, may be where the separatist viewpoint got its start. According to the separatist thesis, privacy and competition law are complementary but do not overlap.[4] The fundamental contention is still that adding privacy considerations to competition law analysis would be confusing, particularly when using the consumer welfare criterion. The approach of strict separation between competition law and data privacy law has been a dominant view in the European Union, which has been reluctant to accept privacy effects in the EU competition law.[5] The integrationist strategy, on the other hand, accepts the integration of privacy within the established framework of competition law.[6] Considering both price and non-price elements could increase consumer welfare.[7] The integrationist approach shows a tight relationship between competition law and privacy-based competition where there is evidence that

[2] Maureen K. Ohlhausen & Alexander P. Okuliar, Competition, Consumer Protection, and the Right (Approach) to Privacy, 80 Antitrust L.J. 121 (2015). Case C-235/08 *Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios* ECR I-11125. [2006]
[3] James C. Cooper, Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity, 20 Geo. Mason L. Rev. 1129, 1146 (2013)
[4] Ohlhausen & Okuliar (n 2).
[5] Viktoria HSE Robertson, ;Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' [2020] Common Mark. Law Rev. 161, 166.
[6] E M Douglas, The New Antitrust/Data Privacy Law Interface (2021) YLJ 647.
[7] See for example: Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 695 (1978)

businesses compete to offer more or less privacy to their customers.[8] One might take into account a hypothetical merger of two internet-based businesses to properly illustrate this. If these businesses compete to offer various levels of privacy before the merger, the evaluation may consider whether the merger significantly limits the privacy options accessible to customers after the merger. The integrationist approach would examine if a decline in privacy as a quality result in less competition.[9]

However, it is acknowledged that the relationship between competition law and data privacy law is complex, especially in the digital markets, where the acquisition of personal data plays a prominent role in business models. In fact, more integrative considerations have attempted to be developed within traditional competition law that focuses on whether data privacy concerns should be directly considered. It remains impossible not to argue that competition law may consider negative effects on privacy, if any direct privacy infringement also introduces negative effects on compiler welfare. Hence, the data-collecting practices might introduce potential negative privacy effects that were considered as a part of the non-price element of quality of a digital products and/or services. The notion of "privacy as quality" is the one that has been expressed the most about the connection between privacy and competition. In *Microsoft/Yahoo!*,[10] the Commission stated that quality becomes a crucial factor in the competition when a product is supplied for free. The "privacy-as-quality" idea considers a rise or reduction in privacy in situations where privacy works as a characteristic of quality impacted by market competition. The Commission has acknowledged this justification in the mergers of *Facebook/WhatsApp* and *Microsoft/LinkedIn.*[11] Similarly, the competition commissioner acknowledged in 2016 that there may be room for competition law enforcement in situations where only a small number of companies controlling data are required to satisfy consumers, as competition law may give them the power to oust rivals from the market and take advantage of consumers.[12] A recent opinion from AG Rantos suggested that a GDPR incidental consideration would be allowed for competition law analysis. This is only possible if the GDPR

[8] Frank Pasquale, Privacy, Antitrust, and Power, 20 Geo. Mason L. Rev. 1009, 1009 (2013).
[9] See Statement of Federal Trade Commission Concerning Google/DoubleClick, FTC File No. 071-0170, at 2 (F.T.C. Dec. 20, 2007)
[10] Case No COMP/M.5727 – *Microsoft/Yahoo!* OJ L 24, 29.1.2004, para 101
[11] Case M.8124 *Microsoft/LinkedIn* [2016] C(2016) 8404 final; Case M.7217 *Facebook/WhatsApp* [2014] OJ C 417/4.
[12] Speech of Competition Commissioner Vestager, 'Competition in a big data world '(2016) *DLD 16 Munich*, 17 January 2016, <https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big- data-world_en.> accessed 10 October 2019.

is integrated into a larger range of the economic and legal circumstances surrounding the conduct.[13]

Data is used by digital platforms to enhance the quality of their services and their appeal to both current and potential clients. Yet, online platforms support the status quo in online marketplaces by requiring it using unclear and misleading wording in privacy rules and unjust business practices. Given that customers were ignorant of Facebook's data analysis procedures, the BKA case against Facebook is an intriguing illustration of an effort to conceptualise unfair business practices from a B2C perspective. They increase the informational asymmetry by keeping customers in the dark about the privacy-related repercussions of using and accessing their online services and products. Competition enforcement may ensure that customers may make informed decisions about the goods and services they choose by encouraging competition in the markets. Increased or diminished privacy protection strategies by Big Tech corporations are two ways that privacy may connect with or affect the competitive theory of harm. Requiring user authorization for data acquisition is one aspect of greater privacy protection (this is Apple's tactic). The BKA's Facebook case has drawn attention to this justification. When more personal data is collected, the dominant position of online platforms may be strengthened, making it possible for consumers to be the well-taken advantage of by being offered "zero pricing" in terms of financial transactions.

As a result, data collecting continues to strengthen platforms' commercial dominance even under privacy restrictions. Large amounts of data alone are insufficient. Any targeting is constrained without user post-ad exposure behaviour and user interests or demographics. The data must be linked to a user using identifiers like cookie IDs or users' IP addresses to be recorded as accurate and useful information. The question of whether these pro-user and pro-privacy developments could strengthen the fallacy of the consumer's choice and serve as a front for more data collection and user exploitation remains.

3. Google Privacy Sandbox and Apple's ATT: a few words on the developments

This section discusses the recent developments of Google's Privacy Sandbox and Apple's ATT, which arguably introduce better privacy protection for users. Google and Apple recently

[13] Case C-252/21 *Meta Platforms and Others* ECLI:EU: C:2022:704, para 23.

changed their privacy policies, which may impact the products they offer. Both initiatives aim to limit third-party cookies, that allow for third-party technologies to track digital users with their consent. Such products 'upgrade' of this essence could impede third-party advertisers' ability to track online users and produce advertisements. Google's Privacy Sandbox and Apple's ATT proposals, as well as their broader implications for competition law and privacy, are predicted to keep regulators busy for years to come, as they could also raise privacy and antitrust concerns. As explained by Google in the UK Competition and Markets Authority's (CMA) review documents, the proposed privacy-related change allows: "to treat [users] as one consistent identity whenever and wherever we [Google] see them."[14]

Any changes to Google's and Apple's privacy policies may have ramifications for ecosystem participants. This, in theory, allows them to act as de facto privacy regulators. Importantly, such power could typically extend beyond the GDPR and any privacy law, with different operational opinions, with the GDPR leading a discretionary approach to compliance. However, Google's and Apple's pro-privacy policy amendments, which limit third-party tracking, do not imply that user tracking will be eliminated: both initiatives do not prohibit the collection and use of first-party data for targeted advertising. This article turns to focus on the Google Privacy Sandbox, which has been widely assessed by competition authorities.

The CMA expressed concerns about Google's Privacy Sandbox and eventually launched a formal antitrust investigation, aiming "to ensure that both privacy and competition concerns can be addressed as the [Privacy Sandbox] proposals are developed."[15] The CMA investigation was fundamental of a competition law nature, focusing on the level of concentration in the market for digital advertising and search in Google's ecosystem at the expense of the competitor. Google's Privacy Sandbox aims to improve user experience and privacy while maintaining an ad-supported business model. The attempt to narrow the model of user identification, however, may introduce exploitative concerns for digital users. It may be difficult to confront exploitative practises in digital markets. As such, this article introduces two elements that could bring exploitation of personal data.

[14] CMA, 'Online Platforms and Digital Advertising Market Study' (July 2020) < https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> accessed 15 November 2022., Appendix F: the role of data in digital advertising, para 133.
[15] CMA, 'CMA to investigate Google's 'Privacy Sandbox 'browser changes' (Press release, 8 January 2021) <https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser- changes> accessed 20 June 2022.

To begin, Privacy Sandbox hinders third-party cookies but does not constrain online tracking. In other words, Google will keep going to have access to a huge amount of user data from services such as Gmail, Google Maps, and the Google search engine, which could be a lucrative source of ad customisation.[16] This phenomenon could lead to pervasive surveillance, which is the collection of data from users participating in a specific network by the device used to participate in such networks.[17] Companies like Facebook and Google may be able to collect even more data. Surveillance on such platforms, in my opinion, could cause exploitative harm to society and online users.[18] The Privacy Sandbox interface has no effect on such procedures, which could take place on popular online services. Geradin suggested that Google emerged unconcerned regarding online tracking.[19] Google's focus on third-party tracking, which allows for the collection of data from sources beyond the platform, could divert attention from Google's and Facebook's tracking procedures. As enhanced data collection provides a competitive advantage over competing intermediaries, Google and Facebook may be able to be assertive in restricting the flow of information among different ad tech companies.[20] Google and Facebook do not display responsiveness when balancing GDPR-enacted fundamentals, which makes it more difficult for Google and Facebook to use data collected from their operated substitutes for any of their ad tech options; this could only be achieved by acquiring a precise consent for that use. In such instances, the companies' preferences could diverge from data protection worries. In this case, digital firms' interests may differ from ensuring data protection for their users'. If digital firms, such as Google, were involved in ensuring their users' privacy, they would use the CMA's suggested purpose limitation principle.[21] Google's core strategy is based on profit maximisation. Equally, it would be cynical to anticipate Google to depend on data minimisation when Privacy Sandbox could introduce opportunities for Google to capture more data, which could become a lucrative origin for Google's ad personalisation.

---

[16] Ben Thompson, 'Digital Advertising in 2022 '(*Stratechery*, 8 February 2022) <https://stratechery.com/2022/digital- advertising-in-2022/> accessed 6 November 2022.
[17] Sally Shipman Wentworth, 'Pervasive Internet Surveillance – Policy ripples' (*Improving Technical Security*, 26 June 2014) < https://www.internetsociety.org/blog/2014/06/pervasive-internet-surveillance-policy-ripples/> accessed 6 November 2022.
[18] On this point, see: Neil M Richards, 'The Dangers of Surveillance' [2013] Harv L Rev 1934, 1952-58.
[19] Damien Geradin, Dimitrios Katsifis, Theano Karanikioti, 'Google as a *de facto* privacy regulator: analysing the Privacy Sandbox from an antitrust perspective' [2021] European Competition Journal 617. 644.
[20] CMA Online Platforms and Digital Advertising Market Study (n 14), Appendix M: intermediation in open display advertising, para 520.
[21] 'CMA to investigate Google's 'Privacy Sandbox' (n 15)

Second, the change to the Privacy Sandbox could be perceived as an unfair term of a contract with Google under Article 102(a) TFEU, and result in self-referencing of Google's tech solutions (operated and owned by Google). Google's pro-privacy policy amendment may have a significant effect on users, notwithstanding the fact that the policy change is ambiguous and difficult to estimate. This article suggests that Google's introduction of the Privacy Sandbox incentive is a two-sided phenomenon. On the one hand, Privacy Sandbox eliminates cross-site tracking, which enhances the quality of privacy creation. This could be regarded as a consumer welfare gain. However, such an advantage may well be restricted since Privacy Sandbox does not reduce surveillance on popular digital platforms such as those operated and owned by Google. Privacy Sandbox, on the other hand, leads to the exclusion of less relevant advertising. This undoubtedly equates to a loss of welfare for customers who value relevant advertisements.[22] The Privacy Sandbox interface could also restrict data consumption, with users having a limited access to free content. Google has been admonished for exploiting its market dominance to prefer its own services. Of course, Google's conduct could distort competition; however, Google may attempt to justify this through privacy issues based on the efficiency defence, relying on a positive competition effect that the third-party cookie ban may support innovation instead of harm consumer choice.

To address the concerns of the CMA, Google introduced a series of commitments to ensure that the implementation of the Privacy Sandbox would not result in distortion of competition in the digital advertising market. Google aims to take several factors while designing, and implementing the Privacy Sandbox, which includes: (i) the impact on competition, (ii) Privacy Sandbox's impact on consumers' data privacy, (iii) technical feasibility, (iv) the impact on Google's user experience over securing their privacy. Google remains transparent over its proposed developments and aims to publicly announce that its design is going to not distort the competition in the digital market. Google's proposals remain based on clear principles — Google will not develop, design, and implement its Privacy Sandbox in a manner that distorts competition and impose unfair terms on its users. In addition, the CMA aims to remain closely involved in the development of the Privacy Sandbox to ensure that Google develops their interface in line with the offered commitments. Importantly, before running a final comprehensive test of the Privacy Sandbox, the CMA will have the power to ask Google for

[22] CMA Online Platforms and Digital Advertising Market Study (n 14), Appendix G: the role of tracking in digital advertising, para 378.

any additional modification to ensure that Google has indeed considered proposed commitments that impact competition and privacy.

3.1 Efficiency defence: generally

Efficiency defences justify the anticompetitive business practice when they introduced positive competitive effects.[23] The nature of efficiency defence has been assessed in the Microsoft case, which concerned Windows Media Player being tied up to its operating system. Microsoft defended its conduct, arguing that tying up Windows Media Player with its system resulted in cost-savings, as consumers would no longer be required to set up a different channel for media player distribution. As a result, consumers would face a decrease in price, and would spend less time installing an alternative media channel. Yet, the Commission held the efficiency argument was potentially irrelevant, based on its reasoning that the costs of the software remained low and could be replaced with little effort. Instead, the Commission focused on the different matters of the proceeding, including consumer choice and innovation rather than efficiencies. Free digital services and products can be disseminated without any user effort. There is a major difference between economics and EU competition law when it comes to weighing efficiency standards: economics considers social welfare,[24] while EU competition law places an emphasis on consumer welfare.[25] Enforcement authorities also consider other objectives besides economic efficiency. The primary objective of EU competition law is to promote economic integration between Member States.[26] EU's overarching goal was to create a single market, where intra-community trade barriers would be eliminated.[27] According to the case of *Consten and Grundig*, an agreement between undertakings to partition markets along national lines might have compromised the integral market.[28] In his paper, Geradin argued that the practice of the Commission might support such a claim, which emphasizes the application of per se prohibition to different conducts by dominant firms.[29] According to others, the rigid

[23] Anna-Lena Baur, 'Analysing the Commission's Guidance on Enforcement Priorities in Applying Article 102 TFEU — An Efficiency Defence for Abusive Behaviour of Dominant Undertakings? '(2012) 19 (3) Maastricht Journal of European and Comparative Law 1.
[24] Simon Bishop, David Walker, *The Economics of EC Competition law — Concepts, Application and Measurements* (2nd ed, Sweet & Maxwell 2002) 20-21, 24.
[25] ibid.
[26] Claus Dieter Elherman, 'The Contribution of EC Competition Policy to the Single Market' [1992] Common Market Law Review 257, 257.
[27] Consolidated Version of the Treaty on European Union, 2010 OJ C 83/01, article 3.
[28] Joined Cases 56/64 and 58/64, *Consten-Grundig* ECLI:EU:C:1966:41
[29] Geradin Damien and Kuschewsky Monika, 'Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges' (2014) 37 World Competition 69.

and formalistic approach of the EU indicated that it was not capable of meeting future innovation needs.[30]

The latest case of *Google (Shopping)* has provided a judicial interpretation of the efficiency argument.[31] The *Google (Shopping) case's* judgement elaborated on the efficiency treatment in the context of the abuse of dominance, building on the analytical framework established in *Post Danmark*, where the Court of Justice of the European Union (hereinafter: CJEU) established that the efficiencies must be pictured regarding their "...actual existence and their extent…"[32] *Post Danmark* established the need for a causal link between the alleged improvement and the anticompetitive conduct. The CJEU insisted on the benefits of consumer choice, demonstrating that any efficiency benefits emanating from the conduct in question should not lead to harmful competition in that market.

The case law seems to show that efficiency arguments are two-fold. First, efficiency arguments shouldn't be broad, theoretical, or ambiguous, and they should not rely on businesses' commercial interests.[33] The CJEU's approach may be quite symmetrical in light of the latter point because actual or potential anticompetitive effects must be demonstrated beyond purely hypothetical considerations like efficiency.[34] The CJEU appears to follow a strict consumer welfare approach,[35] considering that a dominant undertaking could not protect its commercial interest. Also, the CJEU established a system of pseudo-hierarchies while balancing the efficiency arguments.[36] Suppose that, in *Google (Shopping)*, the CJEU indicated that generating efficiency by improving consumer experience did not justify Google's anticompetitive conduct, as the conduct materialising the improvement led to harming competition by reducing shopping services available to consumers.[37] Once more, the CJEU choose to safeguard consumer choice over welfare increases. In general, it may be enough to assume that increased consumer welfare justifies anticompetitive behaviour. Increases in

[30] James Ponsoldt & Christopher David, ''Comparison between U.S. and E.U. Antitrust Treatment of Tying Claims against Microsoft: When Should the Bundling of Computer Software Be Permitted' (2007) 27 Northwestern Journal of International Law & Business 421.
[31] Case T-612/17, *Google (Shopping)* [2021] ECLI:EU:T:2021:763.
[32] Case C-209/10 *Post Danmark A/S v Konkurrencerådet* ECLI:EU:C:2012:172
[33] *Google Search (Shopping)* (n 31), para 553.
[34] Case C-23/14, *Post Danmark II* [2015] ECLI:EU:C:2015:651, para 65.
[35] Case T-228/97 *Irish Sugar plc v Commission of the European Communities* European Court Reports 1999 II-02969
[36] Case M.8124 *Microsoft/LinkedIn* [2016] C(2016) 8404 final.
[37] *Google Search (Shopping)* (n 31) para 566-572

consumer welfare do not lead to increased consumer choice in the reverse scenario, rendering the argument unenforceable.[38] Such evaluation reconfirms that EU competition law has still been inspired by ordoliberalism; competition is perceived as a vehicle for ensuring competitive freedom to encourage consumer welfare whilst also preserving open choices.[39]

3.2. Efficiency defence and privacy

Foremost, how, if at all, do role efficiencies influence privacy protection? Is it desirable to maintain privacy risks as a recognisable efficiency argument in EU competition law? In the opinion of this article, the answer should be supportive. The evaluation of privacy concerns in EU competition law comes to fruition in a chronological spectrum ranging from strict separation to apparent integration. Therefore, likely, privacy will indeed be increasingly deemed as an efficiency argument in competition law assessment. There seem to be two reasons for this conclusion.

Firstly, efficiency[40] and innovation[41] are essential for maintaining a healthy market function. Limiting privacy issues as factors that boost efficiency represents a narrow-minded view of innovation. The digital economy illustrates the need for dynamic efficiencies (innovation), stimulating dynamic markets while reducing marginal returns. Competition authorities should not ignore innovation, as it is undeniably a key driver of competition. This is particularly true for platforms that are just starting up. an ecosystem of modules, capable of supporting machines, users, and sectors using data.[42] This feature enables platforms to regulate themselves via code in a Lessigian manner.[43] Platforms commonly manage complex expectations, including increased user privacy levels. Any adjustments to platform practice could correct any market failure. Platform ecosystem amendments, in contrast, should not be viewed as a threat; assuming that any amendment is indeed a harmful act seems unwarranted. The usual criticism

[38] *Microsoft/LinkedIn* (n 36)
[39] Viktoria Roberson, 'Excessive data collection: Privacy considerations and abuse of dominance in the era of big data '(2020) 57 (1) Common Market Law Review 161; Cristina Caffarra & Tommaso Valletti, 'Google/Fitbit review: Privacy is a competition issue '(*VoxEU*, 4 March 2020) <https://voxeu.org/content/googlefitbit-review-privacy- competition-issue> accessed 7 November 2022.
[40] Council Regulation (EC) of 5 February 2004 on Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings (2004/C 31/03) [2004] OJ C 31/5, para 76.
[41] *Guidance on the Commission's Enforcement Priorities in Applying Article 82*
[42] Annabelle Gawer, 'Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age '(2021) Innovation, Organization & Management 1.
[43] Lawrence Lessig, 'Law of the Horse: What Cyberlaw Might Teach '(1999) 113 Harvard Law Review 501.

equates with the debate denouncing the incorporation of non-economic factors in the evaluation of competition law.[44] Some recommendations condemn any attempt to integrate privacy factors into competition law assessment, asserting that its unscientific nature might result in dystopic competition evaluations.[45] As argued in this article, narrow efficiencies would represent uncertainty and could influence politics. Following that, the question of how to foster innovation is discussed using either Arrowian or Schumpeterian presumptions.[46] Simply placed, while contemplating privacy issues in competition law assessment, consumer welfare and efficiency may well be interconnected. With the implementation of the EU Charter, the Commission is obligated to enable invasions of privacy.[47] Due to a reluctance to intervene in cases that involve direct excess pricing harm, there are no explanations why end-user privacy should serve as a means for competition authorities to act.[48] The question suggests that the gap is not inevitably whether the implementation of competition law is insufficient in evaluating privacy concerns, but that the problem resides within the GDPR implementation due to a lack of adequate regulation. Since competition law should not be extended beyond its natural limits, public policy should not be based on an evaluation of efficiency and competition. This would appear to suggest that market mechanisms, as well as competition law, are inadequate in promoting a high degree of privacy.

Second, if we presume that privacy considerations could be considered methodically by competition analysis, then integrating privacy would necessarily require a coherence perspective. It is inappropriate to consider the negative facets of privacy while excluding any counterpoints predicated on the same. Similarly, the EU is enduring a digital and green transition.[49] Recently, the Commission forbidden a manufacturer's contract that restricted the advancement of less-polluting emission systems.[50] However, there is evidence of a possible conflict between competition law and sustainable development, as demonstrated by the

[44] William Baxter, 'Responding to the Reaction: The Draftsman's View' (1983) 71 California Law Review 618.
[45] Geoffrey Manne, Dirk Auer, 'Antitrust Dystopia and Antitrust Nostalgia' (2021) Truth on the Market <https://truthonthemarket.com/author/manneauer/> accessed 7 November 2022.
[46] J Schumpeter, *Capitalism, Socialism, and Democracy* (George Allen & Unwin 1954); KJ Arrow, 'Welfare and the Allocation of Resources for Invention' in R Nelson (ed) *The Rate and Direction of Economic Activities: Economic and Social Factors* (NBER Books 2016).
[47] Lamadid A, 'On Privacy, Big Data and Competition Law (2/2) On the nature, goals, means and limitations of competition law '(Chillin'Competition, 2014) < https://chillingcompetition.com/2014/06/06/on-privacy-big-data-and-competition-law-22-on-the-nature-goals-means-and-limitations-of-competition-law/> accessed 6 July 2020
[48] ibid.
[49] Jurgita Malinauskaite, 'Competition Law and Sustainability: EU and National Perspectives' [2022] J Eur Compet 336.
[50] Case AT.40178, *Car Emissions* [2021].

adoption of the revised horizontal guidelines.[51] Yet, there are numerous explanations to start examining similar discussion in terms of competition and privacy. The interconnection of competition law and privacy protection is complicated, and it stretches beyond the field of view of competition law enforcement. The concept of privacy is a social process that has been demonstrated difficult to define.[52] Users rarely have the chance to alter the level of privacy provided by platform providers, as it is inconceivable for customers to start negotiating offered privacy levels. However, as the digital society keeps evolving and new vulnerabilities and threats arise, the connection between data protection and competition law becomes more confusing. At its core, competition law is concerned with market power that could have a negative impact on consumer welfare; the Commission Guidelines determined that consumer welfare is considered through price and other factors including innovation, choice, and quality.[53] This will be examined considering Google's Privacy Sandbox and Apple's ATT initiatives, where this article asserts that both raise concerns about anticompetitive behaviour of excluding rivals and exploiting end users.

It is unclear whether Apple or Google could indeed rationalise their projects as being efficient. Apple blocking third-party apps from accessing data required for app customisation may well be perceived as a refusal to supply, as per *Google (Shopping)* case.[54] In response to the CMA's inquiry, Apple asserted that its company did not engage in third-party tracking.[55] As a result, Apple viewed the changes that affect third-party data collection as being outside the scope of their concern. However, Apple's practice, like Google's Privacy Sandbox initiative, could continue to compromise user privacy. Both infrastructures could correspond to increased first-party tracking, which might correspond to greater market power for Apple and Google in the personal advertising market.

---

[51]Nicole Kar, Lauren O'Brien, 'Greening EU competition law: Commission invites comments on draft revised rules on horizontal cooperation '(*Linklaters Insights*, 9 March 2022) <https://www.linklaters.com/en/insights/blogs/linkingcompetition/2022/march/greening-eu-competition-law_commission-invites-comments-on-draft-revised-rules-on-horizontal-coop> accessed 17 May 2022.

[52] IS Rubinstein, 'Big Data: The End of Privacy or a New Beginning? '[2013] Int Data Priv 74, 78.

[53] Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings [2009] OJ C 45/7, para 19.

[54] Christophe Carugati, 'The Antitrust Privacy Dilemma' (2021) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968829> accessed 7 November 2022; Daniel Sokol & Feng Zhu, 'Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates '(2021) USC Law Legal Studies Paper No. 21-27.

[55] CMA, 'Mobile ecosystems' (2022) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL__.pdf> accessed 2 September 2022.

Moreover, as a potential quality metric, Apple could make the argument that the ATT introduced efficiency gains by proving users' privacy.[56] The fact that many online consumers switched to cross-tacking apps after ATT's introduction could indicate this.

ATT interfaces, as proved by Post Denmark I, demonstrate that consumer choice would not be restricted. ATT, essentially, does not prohibit cross-app tracking at all. Consumers, on the other hand, could benefit more from personalised advertising such as through cross-app tracking because it is free and in a better position to consent to it. Essentially, Apple's ATT does not preclude personal adverts, but it has evolved from the default automatic tracking to offering consumers the choice of giving consent to third-party tracking. Matter of fact, Apple's initiative reinforces the consumer choice concept, in fact, Apple's initiative empowers the consumer choice idea, as reinforced by the cases of *Google (Shopping)*[57] or *Google (Android)*.[58] The choice design architecture behind tracking is that the customer is introduced with an opt-in scenario — and this should not take priority over efficiency justifications. Apple has also taken measures to allow app developers to stimulate consumers for tracking information.

Google's attempts to defend efficiency arguments through its Privacy Sandbox venture appear to be ineffectual. The main reason for this is the theory of harm construction: it is unclear as to if Google could immediately cease utilising third-party tracking to inform its advertising businesses. This could be construed as proof of first-party tracking discrimination, for which Google has already been fined in the EU. Moreover, by removing cookies, Google restricts consumer choice, especially for users who value online advertisements. It is uncertain regardless of whether Google is preparing to launch a different, more equitable alternative with the same level of personalisation. As according to current case law, Google's pro-privacy product improvement may not be justified under the efficiency defence if it reduces consumer choice.

4. Privacy under objective justifications

4.1 Objective justifications: generally

[56] P*ost Danmark A/S v Konkurrencerådet* (n 32).
[57] *Google Search (Shopping)* (n 31)
[58] Case T-604/18 *Google and Alphabet v Commission (Google Android)* OJ C 402, 28.11.2019.

Another method for avoiding liability under European competition law is to depend on objective justifications — external factors which exculpate the exclusionary abuse under Article 102 TFEU.[59] There are, in fact, distinct differences between efficiencies and objective justifications,[60] in certain cases, the presence of these routes enables the avoidance of liability for competition law violations. The debate over objective justification could be viewed as an alternative approach to addressing market failures that excludes a behaviour from breaching Article 102 TFEU.[61] According to the Commission, only a limited number of non-competition policies, as well referred to as external to competition law policies, can be regarded during competition law assessment. The examples of external policies, that are, in fact, non-competition law policies, including the protection of employment,[62] media pluralism,[63] environmental protection,[64] or regional development[65] are considered legitimate factors when applying Article 101(3) TFEU to reviewed agreements. However, the Commission suggested that there may be other methods for assessing concerns that are less restrictive to competition law.[66]

Concerning the assessment of policy coordination, it is important to note that EU competition law does not exist as a standalone statute but is part of a larger framework — the TFEU. Townley and Van Rompuy's work on the influence of external policies on competition law identified four possible outcomes for the collaboration of EU external policies with competition policy.[67] Firstly, Article 346(1) TFEU allows potential external policy value to overshadow

[59] Pablo Ibanez-Colomo, 'The (growing) role of the Guidance Paper on exclusionary abuses in the case law: the legal and the non- legal '(*Chillin' Competition Blog*, 9 February 2022) <https://chillingcompetition.com/2022/02/09/the-growing-role-of- the-guidance-paper-on-exclusionary-abuses-in-the-case-law-the-legal-and-the-non-legal/> accessed 17 August 2022.
[60] Case C-549/10 P *Tomra Systems ASA and Others v European Commission* ECLI:EU:C:2012:221.
[61] Eric Gippini-Fournier, 'Resale Price Maintenance in the EU: In Statu Quo Ante Bellum? 'in Barry Hawk (ed), *International Antitrust Law and Policy* (Fordham 2009).
[62] *See for example*, CJEU, 11 July 1985, *Remia BV vs. Commission*, C-42/84, *ECR*, 1985, p. 2545; CJEU, 29 October 1980, *Van Landewyck vs. Commission*, Joined cases C-209/78 to 215/78 and 218/78, *ECR*, 1980, p. 3125
[63] See for example, Commission Decision of 11 June 1993, IV/32.150 - *EBU/Eurovision System*, 93/403/EEC, *OJ*, 22 June 1993 L179/23.
[64] *See* Commission Decision of 8 December 1983, IV/29.955 – *Carbon Gas Technologie*, 83/669/EEC, *OJ*, 31 December 1983, L 376/17; Commission Decision of 12 December 1990, IV/32.363 – *KSB/Goulds/Lowara/ITT*, 91/38/EEC, *OJ*, 25 January 1991, L 19/25; Commission Decision of 17 September 2001, COMP/34493 – *DSD*, 2001/837/EC, *OJ*, 4 December 2001, L319/1; Commission Decision of 16 October 2003, COMP D3/35470 — ARA; COMP D3/35473 — *ARGEV, ARO*, 2004/208/EC, *OJ*, 12 March 2004, L 75/59.
[65] Commission Decision of 23 December 1992, IV/33.814 - *Ford Volkswagen*, 93/49/EE, OJ, 28 January 1993, L20/14.
[66] Case AT.39984, *Romanian Power Exchange/OPCOM* [2014].
[67] Van Rompuy B, *Economic Efficiency: The Sole Concern of Modern Antitrust Policy* (Kluwer Law International 2012) 227; Townley Christopher, *Article 81 EC and Public Policy* (Hart Publishing 2009) 52-53.

and exclude competition policy. Secondly, if infringements of competition law could be balanced, competition law could indeed act as a complementary procedure. It is mentioned that incidental attention to non-competition law policies could be used to identify competition law violations. If that external, to competition law, policy had not been infringed, there would be no competition law violations. Thirdly, the Treaty introduced a 'policy-linking' or 'cross-sectorial' clauses, which requires competition enforcement to consider other policies in "definition and implementation."[68] The last scenario relates to the silence of the TFEU: it will be for the case law to determine and ensure a consistent interpretation across various policies.[69]

Due to practical issues in its application, the EU competition law approach to objective justifications may be criticised.[70] For instance, Nazzini recommended that there are perceptible practical difficulties in differentiating anticompetitive behaviour from its justifications.[71] Although this point of view may seem to be less relevant in the context of recent developments, the notion of objective justifications continues to remain undiscovered: there are no examples of practice where anticompetitive behaviour could have been objectively justified. The CJEU remains sceptical of anticompetitive behaviour serving as a public goal,[72] demonstrating that private enterprises are unsuited to consider the objectives within the purview of public regulators.[73] In other words, EU competition law does not regard such regulatory vigilance as beneficial.

4.2. Privacy as an objective justification

This section examines the treatment of privacy as an objective justification considering the preceding analysis, arguing that it is still possible that digital enterprises will use pro-privacy incentives to exonerate themselves from anticompetitive liabilities.

In the case of privacy protection, neither national nor EU competition law recognises the general obligation to safeguard privacy in the proactive implementation of Article 102 TFEU.

---

[68] *Townley* (n 67) 53.
[69] CJEU, 6 October 1982, *Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health*, 283/81, ECR, 1982,
[70] Renato Nazzini, 'The Wood Begun to Move: An Essay on Consumer Welfare, Evidence and Burden of Proof in Article 82 cases '(2006) 4 European Law Review 518.
[71] Case C-53/03, *Syfait and Others* [2005] ECLI:EU:C:2004:673, Opinion of AG Jacobs, para 72.
[72] Case T-30/89, *Hilti v Commission* [1991] ECLI:EU:T:1991:70, para 118.
[73] Niamh Dunne, 'The Role of Regulation in EU Competition Law Assessment '(2021) LSE Legal Studies Working Paper No. 09/2021

In *Asnef-Equifax*, the CJEU rejected the interplay between competition law and data protection rules by highlighting that data protection law falls outside the purview of competition law.[74] Despite the widespread belief that the relationship between competition law and privacy is complementary, the relationship between competition and data privacy is far more complex and nuanced. This thesis acknowledges that the intersection of competition law and privacy is novel. It is critical to understand that competition law and data protection law are two distinct and separate regimes. However, data protection (and privacy protection) and competition policy share fundamental concerns and approaches to mitigating unfairness by introducing and imposing obligations on those with market power. Due to the relationship between sector-specific regulation and competition law, referencing privacy as a ground for objective justification could be problematic. In AstraZeneca, the Court discussed how compliance with other legal orders has no impact on whether an undertaking has abused its dominant position.[75]

In this regard, any violation of other legal orders does not automatically imply a violation of competition laws. According to this reasoning, it would be impossible for a dominant undertaking to seek justification for its anticompetitive behaviour by citing compliance with data privacy legislation such as the GDPR. Such reasoning appears plausible because it avoids extending competition law rules to capture conducts and harms that are not covered by competition law. However, recent case law appears to dull the problem. For example, in *Lietuvos gelezinkeliai,* the General Court argued that legislative measures are capable of influencing competition law analysis.[76] Furthermore, the case of *Slovak Telekom* emphasised that "...a regulatory obligation can be relevant for the assessment of abusive conduct..." where an undertaking is subject to specific sectoral obligations.[77]

Here, this article demonstrates a tension between these judgements from the perspective of privacy consideration. To begin, under *AstraZeneca*, Article 102 TFEU disregards an undertaking's position and the regulatory regime in question. *Slovak Telekom* and *Lietuvos gelezinkeliai* recently pointed to an apparent relevance of a regulatory regime in question for the purposes of Article 102 TFEU applicability. However, it is unclear whether such a

[74] *Asnef-Equifax* (n 2).
[75] Case C-457/10 P, *AstraZeneca v Commission* [2012] ECLI:EU:C:2012:770, para 132.
[76] Pablo Ibanez-Colomo, 'GC Judgment in Case T-814/17, Lithuanian Railways – Part I: object and indispensability '(*Chillin' Competition Blog*, 1 December 2020) https://chillingcompetition.com/2020/12/01/gc-judgment-in-case- t%E2%80%91814-17-lithuanian-railways-part-i-object-and-indispensability/ accessed 26 March 2022.
[77] Case C-165/19 P, *Slovak Telekom* [2021] ECLI:EU:C:2021:239, para 57.

reconciliatory reading presupposes that a regulatory context could be part of an anticompetitive context. As per AstraZeneca's judgement, we should disregard any potential regulatory breach as part of the competition law assessment, considering breach data privacy law to be irrelevant for competition law purposes. Conversely, in *Google (Shopping) case*,[78] the Court considered the external-for-competition-law-policy for the sake of completeness of assessment. This stage is further complicated by AG Rantos' opinion that incidental considerations of the external-for-competition-law-policies may be relevant, as competition law would not exist if that policy was not violated.[79] As a result, in order to consider the impact of a regulatory regime on the competition assessment of the activity of a dominant undertaking, the latter does not need to be subject to that regime.

It is argued here that there are significant implications for the role of privacy as objective justification. If we assume that *AstraZeneca*'s approach is still appropriate, Apple and Google should not respond to GDPR compliance arguments to avoid anti-competitive scrutiny. In this regard, a theory of harm should not be established based on an infringement of other legal rules. In other words, even if the development of the digital economy has increased competition authorities' interest in privacy-related theories of harm, this should not be construed as an expansion of the competition legal order to that of other areas of law, such as data protection, for the simple reason that competition law relates to addressing harms caused by market failures that undermine market functioning. However, the assumption here is that, considering recent developments in legal cases, the Court could consider privacy-related harms when they influence the theory of harm - and thus the Court should consider them when scrutinising claims of objective justifications.

To elaborate, if a dominant undertaking is found to be in violation of Article 102 TFEU, the undertaking may: 1) argue that its conduct is competitively beneficial; or 2) demonstrate that its conduct is incapable of demonstrating anticompetitive effects.[80] In this regard, assuming that the conduct was pro-competitive, such a situation would constitute an ancillary restraint.[81] However, if a company claims that its anticompetitive behaviour is proportionately pursuing

[78] *Google Search (Shopping) case* (n 31)
[79] Case C-252/21, *Request for a preliminary ruling, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)* ECLI:EU: C:2022:704, Opinion of AG Rantos
[80] Pablo Ibanez-Colomo, 'Anticompetitive Effects in EU Competition Law '(2021) 17 (2) Journal of Competition Law & Economics 309.
[81]Case T-112/99 *Métropole Télévision (M6) v Commission* EU:T:2001:215; Case T-111/08 *Mastercard v Commission* EU:T:2012:260.

non-economic goals, the *Wouters* case suggests that such behaviour cannot be viewed as intersecting ideas.[82] As a result, the question remains whether platforms can claim that their anticompetitive behaviour of infringing (or promoting) privacy is pro-competitive. The answer should continue to be negative. The question should be answered through the involvement of government power as to whether it is legitimate to pursue non-economic considerations. Accordingly, Google and Apple can only rely on their non-economic considerations if they are granted regulatory powers. This conclusion might still be questionable as EU competition law does not see such regulatory vigilantism as complimentary. In the context of the DMA, Google, which is unquestionably a gatekeeper, will unlikely be granted any extra degree of authority.[83]

When the cases of ATT and Privacy Sandbox are discussed, their relationship with an apparent objective justification remains blurry. As previously stated, EU competition law does not view such regulatory vigilantism favourably. As a result, this article believes that accepting privacy protectionism as an objective justification is still weak. Furthermore, the DMA makes no provision for gatekeepers to avoid liability for increased privacy protectionism. Regulatory considerations have been deemed important in justifying the existence of harm theories under Article 102 TFEU. Furthermore, in EU competition law, there may have been recognised regulatory compliance to inform the assessment of a long-running anticompetitive case. At the time of writing, it is unclear how the Commission will decide to enforce actions against undertakings that promote product privacy as an objective justification for anti-competitive behaviour.

5. Conclusion

This article considered the relationship between competition law and data privacy. However, it focused on a different side of the debate — justifications for increased privacy protection for otherwise anticompetitive conduct. In other to justify such findings, this article discussed Google Privacy Sandbox and Apple ATT's initiatives, which limited third-party cookies. Firstly, this article assessed efficiencies and privacy concerns. Efficiency defences justify the anticompetitive business practice when they introduced positive competitive effects. Firstly, efficiency and innovation are essential for maintaining a healthy market function. Limiting

[82] Case C-309/99 *Wouters v. Algemene Raad van de Nederlandse Orde van Advocaten*, [2002] E.C.R. I-1577.
[83] *DMA*, Article 3.

privacy issues as factors that boost efficiency represents a narrow-minded view of innovation. If we presume that privacy considerations could be considered methodically by competition analysis, then integrating privacy would necessarily require a coherence perspective. It is inappropriate to consider the negative facets of privacy while excluding any counterpoints predicated on the same. It is unclear whether Apple or Google could indeed rationalise their projects as being efficient. Apple blocking third-party apps from accessing data required for app customisation may well be perceived as a refusal to supply. Apple's practice, like Google's Privacy Sandbox initiative, could continue to compromise user privacy. Both infrastructures could correspond to increased first-party tracking, which might correspond to greater market power for Apple and Google in the personal advertising market. Another method for avoiding liability under European competition law is to depend on objective justifications — external factors which exculpate the exclusionary abuse under Article 102 TFEU. As ATT and Privacy Sandbox are discussed, their relationship with an apparent objective justification remains blurry. As previously stated, EU competition law does not view such regulatory vigilantism favourably. As a result, this article believes that accepting privacy protectionism as an objective justification is still weak. At the time of writing, it is unclear how the Commission will decide to enforce actions against undertakings that promote product privacy as an objective and efficient justification for anticompetitive behaviour.

The Omission of Anabolic Steroid and IPED Abuse in Fitness Industry Discourse: Seeking a Regulatory Approach to Combat this Online Harm

Melanie Kay McLaughlan

1. Introduction

Anabolic steroid and IPED[1] abuse have been prevalent in professional bodybuilding for decades. Worryingly, an alarming number of the public are now injecting these drugs without professional oversight[2] to achieve a "perfect" physique[3] [4]. Statistics show that around 200,000 adults in the UK[5], and 3% of high school boys in America[6], are using steroids, although these figures are believed to be underestimated when considering an unwillingness to disclose. The main motivation for the use of IPEDs[7] is body image.[8] Steroids are classified as an addictive substance that cause severe psychological and physical effects[9] to the detriment of the individual, which may also result in harm to others[10] due to the link between anabolic steroid use and criminal behaviour[11] (e.g., domestic violence[12]) and thus contributory to an increasing government expenditure in the UK. They are illegal to sell, distribute and possess in most

[1] Image and Performance Enhancing Drugs
[2] Phillip O'Connor, 'Doping is now a public health issue, conference told' (*Reuters*, 22 September 2012) <Doping is now a public health issue, conference told | Reuters> accessed 5 December 2022
[3] Steven Morris 'Up to a million Britons use steroids for looks not sport' (*The Guardian*, 21 January 2018) <Up to a million Britons use steroids for looks not sport | Health | The Guardian> accessed 9 November 2022
[4] Katinka van de Van & Kyle J.D. Mulrooney 'In a bid for the perfect profile pic, young men are increasingly turning to steroids' (*The Conversation*, 23 June 2016) <https://theconversation.com/in-a-bid-for-the-perfect-profile-pic-young-men-are-increasingly-turning-to-steroids-60874> accessed 9 November 2022
[5] Home Office, 'Drugs Misuse: Findings from the 2018/19 Crime Survey for England and Wales' (*Home Office*, 19 September 2019) <Drug misuse: findings from the 2018 to 2019 CSEW (publishing.service.gov.uk)> accessed 5 December 2022
[6] O'Connor (n 2)
[7] Steven Morris 'Up to a million Britons use steroids for looks not sport' (*The Guardian*, 21 January 2018) <Up to a million Britons use steroids for looks not sport | Health | The Guardian> accessed 9 November 2022
[8] Katinka van de Van & Kyle J.D. Mulrooney 'In a bid for the perfect profile pic, young men are increasingly turning to steroids' (*The Conversation*, 23 June 2016) <https://theconversation.com/in-a-bid-for-the-perfect-profile-pic-young-men-are-increasingly-turning-to-steroids-60874> accessed 9 November 2022
[9] NHS, 'Anabolic Steroid Misuse' (*NHS*, 13 April 2022) <https://www.nhs.uk/conditions/anabolic-steroid-misuse/> accessed 14 November 2022
[10] Brian Corrigan AM, FRACP, FACRM, 'Anabolic steroids and the mind' (1996) 165(4) MJA <https://onlinelibrary.wiley.com/doi/epdf/10.5694/j.1326-5377.1996.tb124932.x> accessed 9 November 2022
[11] Ryan C.W. Hall, Richard C.W. Hall & Marcia J. Chapman, 'Psychiatric Complications of Anabolic Steroid Abuse' (2005) 46(4) Psychosomatics <https://www.sciencedirect.com/science/article/pii/S0033318205700669> accessed 9 November 2022
[12] Carrie Mullen, Benjamin J. Whalley, Fabrizio Schifano & Julien S. Baker 'Anabolic androgenic steroid abuse in the United Kingdom: An update' (2020) 177(10) BJP <https://bpspubs.onlinelibrary.wiley.com/doi/10.1111/bph.14995> accessed 9 November 2022

jurisdictions.[13] This paper seeks to provide a legal solution to the harm (when defining harm as an act which causes harmed states or conditions in people[14]) inflicted upon individuals by fitness influencers who intentionally post content on social media platforms that omits their anabolic steroid and IPED abuse, disseminating a discourse that they have achieved their physiques "naturally" (solely using exercise, diet, and natural supplements).[15] Content assigned to users by the algorithm,[16] in combination with influencers who "exert commercial and non-commercial influence"[17] over their audience, frames the platform user's perception of the world. Although influencers[18] raise significant consumer protection issues too,[19] this paper focuses exclusively on how far the platform's responsibility should extend in governing the public's consumption of content that could be harmful.[20] In doing so, the role that platform architecture plays in exploiting the vulnerabilities of platform users will also be considered.

2. Law 1.0: Attempting to regulate technology via tort law

Fitness and bodybuilding content generates two fundamental issues because of the implicit promotion of steroid and IPED use:

1) Harm caused to social media users who are unaware of and not educated on the steroid and IPED abuse in the fitness industry. They are exposed to imagery of unattainable body standards and try to achieve these standards naturally but fail to do so, which can result in body dysmorphic disorder.[21] This audience may be influenced by the

[13] For example: Anabolic Steroid Control Act of 2004 in the UK and SARMs Control Act of 2019 in the USA. Whilst they are illegal to both sell and possess in the USA, they are only illegal to sell in the UK.
[14] Joel Feinberg, *The Moral Limits of the Criminal Law Volume 1: Harm to Others* (1st edn, OUP 1984)
[15] Noel Deyzel, 'Why I'm open about my steroid abuse' (*YouTube*, 3 July 2021) <(684) Why i'm open about my steroid use. - YouTube> accessed 13 December 2022
[16] Barrie Sander, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law' [2021] 32(1) European Journal of International Law
[17] Digital, Culture, Media, and Sport Committee, 'Influencer culture: Lights, camera, inaction? Twelfth report of session 2021-2022' (*House of Commons*, 26 April 2022) < Influencer culture (parliament.uk)> accessed 26 November 2022
[18] See for example, Alex Hammer, 'Super-buff influencer 'Liver King' -famed for his natural physique and caveman-lifestyle – is blasted for using $12,000 of steroids a month by rival fitness guru' (*The Daily Mail*, 30 November 2022) <Liver King' who became famous online for his natural physique accused of steroid use | Daily Mail Online> accessed 5 December 2022
[19] Liver King, 'Liver King Confession… I Lied.' (*YouTube*, 2 December 2022) <(673) Liver King Confession... I Lied. - YouTube> accessed 5 December 2022
[20] Luke Price, 'Platform responsibility for online harms: towards a duty of care for online hazards' (2021) 13(2) Journal of Media Law 238
[21] NHS (n 9)

appearance of the influencer to the extent that they may use steroids and IPEDs once they become knowledgeable of this drug use within the community.

2) Harm caused to social media users who have an awareness of steroid and IPED abuse in the fitness industry. They are exposed to imagery of unattainable body standards and seeing this content frequently normalises substance abuse. Because it is normalised for this audience, they are more likely to participate in this harmful behaviour. In this scenario, the social media audience member can be likened to an enlightened consumer, given that they presume there has been an omission of substance use on the influencer's part; in other words, they are knowledgeable of the information asymmetry that exists between influencer and social media user. This knowledge does not necessarily mean that they do not succumb to the influence, however.

Law 1.0[22] includes tort law because it is founded upon precedent and judicial norms and rules. The tort of negligence aims to establish liability for damages caused.[23] A duty of care can be imposed where there is no direct relationship between defendant and plaintiff. The concept of duty of care builds upon social contract theory; the responsibilities, or obligations, assigned to individuals within a society to benefit the society as a whole.[24] *Donoghue v Stevenson*[25] introduced "the neighbour principle", which states that reasonable care must be taken to avoid acts or omissions that "would be likely" to cause harm to your neighbour. A "neighbour" is defined as an individual directly affected by an act or omission. The entity who owes a duty of care must contemplate how their act or omission would affect the individual before committing said act or omission.[26] The relationship between influencer and audience can be constructed via the neighbour principle as the content is being created directly for the audience. *Bryan v Maloney*[27] set the precedent of "reasonability" of the plaintiff to rely on the knowledge of the defendant. Fitness influencers often market themselves as experts despite their lack of attributable qualifications, and the audience relies upon this information which may be inaccurate or misleading. The influencer could be obliged to use disclaimers in their content, acting as an "exclusion clause"[28] that would void them of liability for the inaccuracy of the

[22] Roger Brownsword, *Law 3.0: Rules, Regulation and Technology* (1st edn, Routledge 2020)
[23] Rachel Mulheron, *Principles of Tort Law* (2nd edn, CUP 2020)
[24] John Locke, *Second Treatise of Government* (1689)
[25] Donoghue v Stevenson [1932] AC 562, 619
[26] ibid
[27] Bryan v Maloney (1995) 182 CLR 609
[28] Mulheron (n 23)

information provided, but this would not address the underlying problem of substance abuse and information asymmetry[29] between influencer and audience.

The reach of duty of care is limited by contributory negligence.[30] It could be argued by the defence that the plaintiff failed to exercise reasonable care to protect their own safety by making an autonomous decision to purchase these prohibited substances. However, if the audience's function is to be influenced by the defendant, is the decision to start misusing steroids and IPEDs entirely autonomous, or is it subconsciously promoted to them?[31] Individuals should not be expected to have perfect comprehension of their environment.[32] Modern case law focuses more on the vulnerability[33] of the plaintiff, which in tort law is described as the plaintiff's inability to protect themselves from harm.[34] More broadly, vulnerability can be viewed as the "social consequences of consumption for different populations in a wide range of marketing contexts",[35] further defined as the consequent powerlessness that arises from "an imbalance in marketplace interactions or from the consumption of marketing messages and products".[36] Not all posts by a fitness influencer are monetized or are directly advertising a product or service, however the content that appears to be simply sharing fitness advice is still contributing to the influencer's overall brand and messaging. The influencer should be thought of as a business, and therefore all content distributed on their platform becomes a marketing message. A consumer's social perception of appearance[37] is likely to affect their individual response to content that they view online (particularly the content of fitness influencers). Consumers, including consumers of content, are expected to be "reasonably well-informed, reasonably observant and circumspect",[38] which

[29] Peng Ma, Jennifer Shang, and Haiyan Wang, 'Enhancing corporate social responsibility: Contract design under information asymmetry' (2017) 67 The International Journal of Management Science <https://browzine.com/libraries/984/journals/5989/issues/8594220> accessed 14 November 2022
[30] Mulheron (n 23)
[31] Martha Albertson Fineman, *The autonomy myth: a theory of dependency* (New Press 2004)
[32] Christine Riefa and Severine Saintier, *Vulnerable consumers and the law: Consumer protection and access to justice* (1st edn, Routledge 2020)
[33] Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20(1) Yale Journal of Law & Feminism
[34] Carl F. Stychin, 'The Vulnerable Subject of Negligence Law' (2012) 8(3) International Journal of Law in Context 353
[35] Stacey Menzel Baker, James W. Gentry, and Terri L. Rittenburg, 'Building Understanding of the Domain of Consumer Vulnerability' (2005) 25(2) Journal of Macromarketing
[36] ibid
[37] M. C. Martin and J. W. Gentry, 'Stuck in the model trap: The effects of beautiful models in ads on female pre-adolescents and adolescents' (1997) 26 Journal of Advertising
[38] Case C-210/96 Gut Springenheide GmbH and Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt [1998] ECR I-4657 , [37]

is an unreasonable assumption to make, and yet this assumption permeates digital marketplaces and platforms.

Attitudes cultivated towards psychiatric harm within tort law doctrine are rooted in the Victorian era, and hence difficult to apply to modern technological advancements. Technology can inflict harm that the law was never previously accounted for nor recognised,[39] and tort law has proven that it can adapt to some technological innovation.[40] Given that platforms host billions of users worldwide with the potential to cause widespread harm, it is likely that a claim of negligence made would trigger more claims and indeterminacy of liability would invoke the floodgates principle, first referred to in the *Victorian Railway v Coultas* case, which feared a wide range of "imaginary claims".[41] In another case, Lord Macmillan acknowledged that the complexity of psychological harm presents questions surrounding the "proper scope of legal liability".[42] The markers of a successful case in this area which "exert dominance"[43] are matters of immediacy and physical contact, which may additionally inhibit a tort law approach to the issue that this paper seeks to address. Further questions concerning the relatability of the parasocial relationship between influencer and user to the existing framework would also need to be addressed to assess suitability. As explored in this section, whilst some elements of the tort law doctrine can be applied to this issue, the overlying framework is most likely not reworkable for these purposes, as judges may be hesitant to rewrite the doctrines maintained within the existing case law, viewing such action as a violation of the separation of powers.

3. Law 2.0: The Online Safety Bill and The Digital Services Act

If tort law cannot be applied to the technology, this forces the creation of new legislation and policy initiatives that specifically target the technology, known as Law 2.0.[44] These legislations

[39] Lyria Bennett Moses, 'Understanding Legal Responses to Technological Change: The Example of In Vitro Fertilization' (2005) 6 Minn JL Sci & Tech 505
[40] Jonathan Morgan, 'Torts and Technology' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP 2016)
[41] Imogen Goold and Catherine Kelly, 'Who's Afraid of Imaginary Claims? Common Misunderstandings of the Origin of the Action for Pure Psychiatric Injury in Negligence 1888-1943' (2021) 138 Law Quarterly Review
[42] Bourhill v Young [1943] AC 92
[43] Lord Steyn, The 8th John Maurice Kelly Memorial Lecture (2001)
[44] Brownsword (n 22)

place a legally obligated duty of care on platforms that didn't formally exist previously. The UK's Online Safety Bill[45] (hereafter, the Bill) focuses on psychological harm, appearing to take inspiration from tort law. It defines "harm" as "psychological harm amounting to at least serious distress",[46] but confusingly it does not define psychological harm, and because there are no formal legal definitions for this term it could apply to a wide range of potential harms depending on the perception of the legislator, which has inspired freedom of expression[47] debates.[48] For this paper, it will be assumed that psychological harm refers to negative impacts upon an individual's state of wellbeing. The "legal but harmful" concept creates another layer of confusion. According to the Online Harms White Paper,[49] content that promotes suicide and eating disorders were promised to fall under the legal but harmful category, but this is not delivered in the resultant Bill. There is also some public discourse surrounding the right to be able to cause harm to yourself. Posting eating disorder content for example can consequently cause harm to others by glamourising that choice and potentially influencing others to participate.

Because the Bill does not identify specific harms to counteract outside of illegal content,[50] it has generated criticism from scholars.[51] The "promotion of drugs" is listed as illegal content in the Bill because drugs are a criminal offence, but this is the first time that legislation has explicitly provided provisions for platforms to prioritise the removal of this content. However, a blanket ban on content that "promotes illegal drugs" would arguably prevent honest discourse and educative content on the subject, depending on the perception of the moderator. This is also a grey area as in the UK steroids are illegal to distribute, but it is not a criminal offence to have steroids in your possession for personal use, whereas in other jurisdictions it is an offence. Ultimately, the primary reason fitness influencers do not disclose their substance abuse is

[45] Online Safety Bill 2022
[46] ibid, s.150 (4)
[47] Joe Mullen, 'Experts Condemn The UK Online Safety Bill As Harmful To Privacy And Encryption' (*Electronic Frontier Foundation*, 23 November 2022) <Experts Condemn The UK Online Safety Bill As Harmful To Privacy And Encryption | Electronic Frontier Foundation (eff.org)> accessed 13 December 2022
[48] Article 19, 'UK: Online Safety Bill threatens freedom of expression and privacy' (*Article 19*, 16 November 2022) <UK: Online Safety Bill threatens freedom of expression and privacy - ARTICLE 19> accessed 13 November 2022
[49] HM Government, 'Online Harms White Paper: Full Government Response to the consultation' (*HM Government*, December 2020) <Online Harms White Paper: Full Government Response to the consultation - CP 354 (publishing.service.gov.uk)> accessed 5 December 2022
[50] Online Safety Bill s.52
[51] Markus Trengove, Emre Kazim, Denise Almeida, Airlie Hilliard, Sara Zannone, and Elizabeth Lomas, 'A Critical Review of the Online Safety Bill' (2022) 3(8) Patterns

economical: fitness influencers are less likely to get sponsors and brand deals if they are open about their drug use. Influencers also want to be perceived by their audience as authentic and relatable. Steroids and IPEDs are a costly habit and therefore are likely unaffordable for a large portion of their audience. There is also shame associated with being a drug user, and steroid and IPED users generally do not believe that they are like other drug users. The psychological harms (e.g., "roid rage") and embarrassing physical side effects (such as shrunken testicles) would likely cause harm to the influencer's reputation as well. The platform may also choose to deal with discussion about steroids and IPEDs as illegal content.

Because steroid and IPED abuse has been declared a global public health problem,[52] it should fall within the scope of the EU's Digital Services Act[53] (hereafter, the Act). This Act has also been influenced by tort law by imposing a duty of care upon platforms, but the Act is more focused on regulating e-commerce than on regulating "psychological harm". The EU equivalent to tort is known as "extra-contractual liability".[54] Unlike the Bill there is not a focus on psychological harm and there is no concept of "legal but harmful". However, the Act does require platforms to monitor risks to public health[55] and "serious negative consequences"[56] to an individual's physical and mental wellbeing, which can be compared to the Bill's "psychological harm" idea. Platforms are required by the Act to assess societal risks,[57] but because this function is self-regulatory this means that platforms decide what risks they deem to be most important in alignment with their values and linked to their terms of service, but an oversight body will be created to ensure transparency.[58] The outcome of these risk assessments remains to be seen, but it will be interesting to see what content platforms identify as harmful to an individual's physical and mental wellbeing. The Act could be improved by directly identifying existing risks and explicitly listing what harms platforms must regulate; currently it gives too much control to the platforms. Similarly to the Bill, the Act enforces compliance through large fines for not removing illegal content (based on the laws of member states).

[52] O'Connor (n 2)
[53] The Digital Services Act Regulation (EU) 2022/2065
[54] Cees Van Dam, 'European tort law' in Christian Twigg-Flesner (eds), *The Cambridge Companion to European Union Private Law* (CUP 2010)
[55] Digital Services Act at fn.53, Article 34(d)
[56] ibid
[57] ibid, (154)
[58] Digital Services Act, Article 40(3)

4. Law 3.0: Social media regulation and addressing as a matter of disinformation

Influencers have the power to "shape and impact" individuals, which requires "bespoke" legal and regulatory frameworks.[59] When the issue requires regulation by technology itself or via technological actors (e.g., social media platforms), either as the sole means of governance or supplementary to Law 2.0,[60] this is known as Law 3.0. Law 3.0 translates the underlying normative view into "practical design", whereby the design would ensure that participants comply with said normative view. A good practical design creates "immediate signals relating to what can and cannot be done"[61] for participants. This paper ultimately proposes to conceptualise this phenomenon as a public health issue caused by disinformation disseminated by influencers, resulting in widespread harm to psychological and physical health. This content can be constituted as disinformation because it is a collective of individuals who are intentionally omitting their drug use and are spreading false information masked as expert advice and content on achieving their physique "naturally".

A core priority of The Act, outside of e-commerce, is combatting the dissemination of disinformation. It asks platforms to prevent the "coordinated disinformation campaigns relating to public health".[62] When conceptualising this issue as a disinformation campaign, it may even have implications for the brands that the influencers are affiliated with as well, given that it is likely that clothing brands such as Gymshark will not want to be affiliated with substance abuse, and supplement brands cannot be affiliated with steroid and IPED users either because it would prove that their products are ineffective, so it is suspected that there are contractual agreements between brands and fitness influencer to not harm the brand's reputation by discussing steroids or IPEDs. Furthermore, the Act requires platforms to combat disinformation that has a "real and foreseeable negative impact on public health".[63] Platforms have their own internal policies on disinformation.[64] Meta removes disinformation that contributes to "imminent physical harm" and reduces the "prevalence" of less threatening

[59] Hettie Homewood, 'Influencer Culture: Filling the Regulatory Gaps' (2022) 33(7) Entertainment Law Review 237
[60] Brownsword (n 22) 4
[61] ibid, 53
[62] Digital Services Act (83)
[63] Digital Services Act (95)
[64] Referred to as "misinformation" in policies: Platforms use this term as a catch-all because it is often difficult to determine intent.

disinformation, aiming to create an online environment that "fosters productive dialogue".[65] Transparency and information sharing in the fitness industry[66]- productive dialogue- would be a crucial step towards combatting the "natural" disinformation trend. Meta achieves this by using third-party fact-checking organisations to empower users to decide what content to trust,[67] which could usefully be employed to combat this type of disinformation too. Crucially, Meta prioritises health disinformation as a primary category of disinformation and cites consultations with leading health organisations to identify harmful disinformation likely to contribute to harm of public health and safety.[68] Meanwhile, Tik Tok, who define disinformation as "content that is inaccurate or false",[69] will remove disinformation "that causes significant harm" to individuals or the public "regardless of intent",[70] unlike Meta who take a more nuanced approach. Twitter's policies have been excluded from this discussion as they are in a state of flux at time of writing.[71] Nevertheless, the existing platform policies and legislation pertaining to disinformation can only be useful if steroid and IPED abuse is viewed as a public health issue by governments too.

The UK strategy for tackling disinformation online,[72] which did not materialise in the Bill aside from a statement concerning the "duty to promote media literacy",[73] is inadequate. As a standalone provision for combatting disinformation in the Bill, this appears to place fault on the platform user for not being educated enough to identify disinformation autonomously. The EU's world-leading Strengthened Code of Practice on Disinformation[74] (hereafter, the Code), supplementary to the Act which requires the employment of "trusted flaggers"[75] with industry knowledge to assess content for disinformation, protects platform users from harm caused by

[65] Meta, 'Misinformation' (*Transparency Centre*, 2022) <Misinformation | Transparency Centre (fb.com)> accessed 5 December 2022
[66] O'Connor (n 2)
[67] Meta, 'How fact-checking works' (*Transparency Centre*, 2022) <How fact-checking works | Transparency Centre (fb.com)> accessed 5 December 2022
[68] Meta (n 65)
[69] Tik Tok, 'Integrity and Authenticity' (*Tik Tok*, 2022) <Community Guidelines (tiktok.com)> accessed 5 December 2022
[70] ibid
[71] Marianna Spring, 'Charities' dismay as Twitter disbands safety group' (*BBC*, 14 December 2022) <Charities' dismay as Twitter disbands safety group - BBC News> accessed 14 December 2022
[72] Department for Digital Media, Culture and Sport, 'Minister launches new strategy to fight online disinformation' (*GOV UK*, 14 July 2021) <Minister launches new strategy to fight online disinformation - GOV.UK (www.gov.uk)> accessed 5 December 2022
[73] Online Safety Bill, 131(4)
[74] The Strengthened Code of Practice on Disinformation 2022
[75] Digital Services Act, Article 22

disinformation. The Code requires signatories[76] to provide tools for users to flag disinformation, access authoritative sources and engage in media literacy initiatives to empower vulnerable users.[77] Commitments for signatories include minimising the risks of actively spreading disinformation,[78] offering users the option to check authenticity of content,[79] and enable users to "make more informed decisions when they encounter online information that may be false or misleading".[80] The trusted flagger approach for the issue explored in this paper specifically may present additional problems, however. This is because the decision-making process would be possibly too subjective in deciding whether to label fitness content for disinformation, given that there is no guaranteed metric to base this on from solely viewing photos, although many would argue that steroid use is easy to identify when considering what is normatively achievable for the human body without the interference of drug use.

The alternative, algorithmic regulation, would present even more issues. Algorithmic regulation[81] aims to manage risk or alter human behaviour through the systematic collection of data within the regulated environment to ascertain a pre-specified goal,[82] which Yeung[83] refers to as a "new system of social ordering". This regulatory approach is risk-based. Algorithmic decision-making is "the use of algorithmically generated knowledge systems to execute or inform decisions".[84] Algorithmic monitoring for this purpose (flagging suspected disinformation by fitness influencers) can only be reactive, not pre-emptive. This approach would absolutely require human moderation as algorithms cannot grasp "the meaning of the law as based on a very specific understanding of human action and interaction".[85] In both cases however, this approach would likely result in claims that certain influencers have been unfairly targeted for their appearance which is based on a belief rather than evidence. Therefore, the only viable approach in tackling this online harm would be generalised labelling such as a "tap for more information" buttons across all fitness content, which would make reference to this

[76] Meta, Twitter and Tik Tok are signatories to the Code
[77] Code at fn.74, Commitment 17
[78] Code at fn.74, Commitment 18
[79] Code at fn.74, Commitment 20
[80] Code at fn.74, Commitment 22
[81] Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12(4) Regulation & Governance 505
[82] Julia Black, 'Learning from Regulatory Disasters' (2014) LSE Law, Society & Economy Working Papers 24/2014
[83] (n 81)
[84] (n 81), 507
[85] Mireille Hildebrandt, 'Algorithmic regulation and the rule of law' (2018) 376(2128) Philosophical Transactions of the Royal Society A 9

disinformation trend that has spread across the fitness community. Targeting bodybuilding content specifically only would push bodybuilding influencers into the general fitness space by refraining from using bodybuilding specific terminology in their content, as a means to avoid this label, and would make this content more mainstream by default. Additionally, it is a misconception that steroids are only used by bodybuilders. It would only be constructive to label all fitness content with verified information links which may also include support and treatment options.

Although I am proposing that algorithmic moderation would not be a suitable solution to moderate this content, this does not mean algorithms do not play a role. In fact, algorithms play a role in proliferating this harm by recommending potentially harmful and misleading fitness content to users based on their actions and behaviours online. This makes the platform user vulnerable and susceptible as a target who has had this content assigned to them in their feed. This digital architecture exploits the power imbalance between content creator and content consumer marketplace.[86] Systemic vulnerability affects all platform users and should be viewed as the norm rather than the exception.[87]

The type of content that would be flagged as disinformation would be content that imparts fitness expertise or advice to the audience. Platforms should monitor over time how influencers may circumvent these measures.[88] The intention behind these disinformation tools would be to create a transparent dialogue surrounding steroid and IPED abuse in the fitness industry and to inform platform users of potential harms so that they can make informed decisions when engaging with this content, which will also increase trust in the platforms. Content that is flagged for disinformation should also link platform users to support pages for both body dysmorphic disorders and substance abuse (concerning psychological and physical harm). The platform would then have to ensure that there are sufficient freedom of expression safeguards in place which allow discussion of IPED abuse to that platform users can successfully spread awareness of IPED abuse as well as sharing treatment and support options. Otherwise, the

[86] BEUC (N Helberger, O Lynskey, H-W Micklitz, P Rott, M Sax, J Strycharz), EU Consumer Protection 2.0, Structured Asymetries in digital consumer markets (BEUC 2021) 17, para 38.
[87] ibid
[88] Ricardo Ribeiro Ferreira, 'Liquid Disinformation Tactics: Overcoming Social Media Countermeasures through Misleading Content; (2022) 16(8) Journalism Practice

concern would be that this useful and informative content would be flagged as disinformation. The role of the trusted flaggers would then become to monitor to ensure that content discussing steroid and IPED abuse openly and that signposted support is not also flagged with this disinformation feature. Overall, this approach allows the content to be posted but attempts to safeguard the user. It remains to be seen how this feature would work in practice. In consumer law, mandatory disclosure, which aims to preserve autonomy,[89] has been viewed by some as a failed consumer protection tactic,[90] given that many do not make use of the information available to them. Overuse of information as a 'transparency' approach, as well as gaps in the law pertaining to the regulation of unfair practices and a lack of sufficient protection for vulnerable consumers are collectively viewed as the primary insufficiencies of consumer protection.[91]

This paper rejects the idea that all users should reasonably be expected to be informed or self-aware enough to make the choice to unfollow fitness influencers and hide related content when they notice that they are developing body image issues. If anything, the algorithm will notice that an individual engages with this type of content and will feed the individual more related content, which can be a difficult to separate oneself from autonomously. Implementing this design to circumvent this issue by proposing it as disinformation disseminated by fitness influencers would be distinctly defining how far the platform's duty of care extends: any choices made after engaging with these disinformation and education tools could then be accepted as autonomous decisions made by individuals and therefore outside the parameters of the platform's liability.

4.1 Brief consideration of the Advertising Standards Agency

Whilst these standards are only applicable to advertisement and marketing of products or services, all content posted by an influencer contributed to their brand's overall marketing

[89] Stephen Breyer (1982), *Regulation and its reform* (Cambridge: Harvard University Press 1982)
[90] O Ben-Shahar and CE Schneider , *More Than You Wanted to Know- The Failure of Mandated Disclosure* (Princeton, Princeton University Press 2016)
[91] Paolo Siciliani, Christine Riefa, and Harriet Gamper, Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making (Oxford: Hart Publishing 2019) 16–55

strategy, as discussed earlier in this paper. In taking this approach, the ASA's CAP Code[92] could potentially be applicable in combatting this specific online harm, or at least in drawing attention to this harm, given that adherence to the Code is voluntary. The Code tackles misleading advertising and marketing, stating that this content must not omit material information.[93] Material information is information that the consumer needs to make informed decisions in relation to a product or service. Again, this comes back to the problem of being able to assuredly identify fitness influencers who use anabolic steroids and IPEDs. However, it is worth considering how unfair commercial practices statutes could be updated to tackle this specific issue, whereby a product or service is not being advertised in the specific content but the content itself constitutes as a marketing message for the overall brand and business of the influencer.

5. Conclusion

The World Health Organization (hereafter, the WHO) declared steroid and IPED abuse as a public health issue[94] and called for cooperation to collectively tackle this harm. This declaration was made ten years ago and virtually nothing has been done since. Because platforms are already consulting with leading health organisations,[95] if this issue were to be made a matter of priority in consultations with platforms, the pressure for change could potentially result in action from social media companies. It may even be possible to achieve this without additional amendments to legislation, as "reputation is a significant form of micro governance"[96] for technological actors, who do not want to be perceived as inherently bad.

Alternatively, there are valuable principles that can be recovered from tort law (Law 1.0) which can help to reshape provisions in the Act and the Bill (Law 2.0). The primary value from tort law that should be maintained is that you can owe a duty of care, not intend to cause harm, and

[92] Advertising Standards Authority, '03 Misleading Advertising' (Advertising Standards Authority, n.d.) <https://www.asa.org.uk/type/non_broadcast/code_section/03.html> accessed 16 January 2023
[93] ibid
[94] O'Connor (n 2)
[95] Meta (n 65)
[96] Andy C Pratt, 'Advertising and creativity, a governance approach: a case study of creative agencies in London.' [2006] 38(10) Environment and planning A: Economy and Space

yet still cause harm. The Act, as the more promising legislation, must be modified to place more of an emphasis on structural issues and collective interests within society.[97] However, Law 2.0 requires the assistance of Law 3.0 to ensure that the provisions of the legislation can be implemented in practice. It is also important to remember that the platform's interests lie with generating advertising revenue, which is why legislation is necessary to enforce platform governance. This paper's proposed conceptualisation of the issue as disinformation, which is rooted in principles of Law 1.0 and is made actionable by Law 2.0, provides a feasible solution to prevent more harm from occurring. The beauty of the Act is that it is a regulatory export; platforms will be cut off from Europe for repeated and severe non-compliance, which would be an unfathomable financial loss for a platform. Whereas increased governance in this area may have economic consequences for fitness influencers, it may also encourage fitness influencers to pivot towards less harmful practices. Although the increased intermediary liability imposed upon platforms by the Act is promising, the impact it will have remains to be seen in practice.

Further studies in this area should analyse the pseudo-labour relations between the influencer and the platform as this will further assist in determining liability. It may be worth turning to online labour marketplaces such as Fiverr and Upwork to deduce a reasonable framework for how platforms can facilitate the influencer's business conduct within the platform.

[97] Rachel Griffin, 'Rethinking Rights in Social Media Governance: Human Rights, Ideology and Inequality' (2022). Available at <https://ssrn.com/abstract=4064738 or http://dx.doi.org/10.2139/ssrn.4064738> accessed 1 November 2022

Volume 9
Issue 2
2022