The Transition from "Free" to Subscription Models in Big Tech

Dr Olga Kokoulina
Assistant Professor, Ph.D., MSc. (Oxford), LL.M., Centre for Private Governance (CEPRI),
Faculty of Law, University of Copenhagen.

Introduction

Throughout the history of communications technology, the promise of openness and democratised access has routinely been followed by waves of consolidation and control. Tim Wu terms this recurring pattern the "Cycle": a process by which emerging technologies move from spaces of experimentation and creativity to tightly regulated areas of commercial control, standardised access, and corporate governance.[1] While each new wave of innovation is often framed as unprecedented, the pattern appears to repeat itself with evident consistency: from telephony and radio to television and, now, the Internet. What is so often introduced as a tool for participation and a means of societal inclusion frequently reveals itself, over time, as a vehicle for "extraction".[2] Advertising often plays a central role in such transformations, acting as one of the means to subside access and promote content creation at first, to become a defining force that shapes the content and conditions of access later.

In light of the historical parallels, to reimagine Big Tech today requires confronting not just the ad-based data-driven business model and its reformulations per se, be they subscription offerings or various forms of tiered-access models. Regulatory scrutiny of these manifestations alone may amount to little more than merely managing symptoms. Rather, the task demands also acknowledging the dominant drivers and infrastructural dependencies that ultimately shape the actual reach and limits of traditional regulatory thinking, and challenges it to seek potential levers within the architecture of this dominant and extractive business model.

This contribution offers an exposé of this point. It focuses specifically on the rise of the "consent or pay" model, which, in essence, represents more of a recalibration than a substantive departure from data-extractive and driven business logic. The emerging regulatory response, though in parts potentially promising, remains largely compartmentalised and tentative, often relying on enforcement patterns and tools that fall short of addressing the scale and logics of the infrastructure they attempt to govern. Instead, this contribution seeks to initiate a discussion that accounts for the affordances and faculties of the infrastructure itself, aiming to identify potential ways to leverage it for regulatory purposes.

A. Advertising

As well documented, advertising has historically functioned not only as a novel revenue stream but as a powerful structural and societal force reshaping entire media ecosystems and redefining the relationship between content, audiences, and institutional arrangements. The narrative of the early era of radio broadcasting in the US provides a case in point. While the decision to allow advertising in American radio broadcasting was not uncontested, it ultimately appeared as an outcome of the interplay of economic and institutional pressures facing the

* The submission is an early draft of a book chapter accepted for publication in the *Cambridge Companion on Big Tech,* prepared as part of the project PROFIT: Gaps and Opportunities in the Corporate Governance of Big Tech Companies, supported by the DFF Inge Lehmann grant (no. 10.46540/2099-00025B; grant recipient: Prof. Andhov).

[1] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Vintage 2011) 6

[2] Julie E. Cohen, *Between Truth and Power: The Legal Cnostructions of Informational capitalism* (OUP 2019) 44

medium in its formative years.[3] Initial objections, opposition, and even hostility reflected a broader concern with the potential of the commercial interests to erode the cultural and educational promise of the radio.[4] However, the costs of maintaining the diverse and often non-commercial broadcasters soon revealed the inherent limitation of the original hardware-based revenue model, which relied primarily on the sale of radio sets. As the initial boom in sales of receivers subsided due to the finite demand from households, the sustainability of the revenue stream came to light. The industry was ultimately confronted with a structural dilemma, in which a publicly administered funding mechanism and advertising as a self-sustaining commercial solution emerged as two principal alternatives.[5] Effectively embracing the latter, American radio broadcasting evolved into a "zero-sum" game for audience attention, where the success of a given radio station became contingent upon its ability to capture and retain the largest possible listenership to attract advertisers.[6]

Decades later, the same dynamics would re-emerge in the digital space of the Internet. Thus, in their original paper describing the foundation for what would later become Google, Larry Page and Sergey Brin explicitly recognised the risks of advertising-based funding models. Arguing that advertising has an undeniable potential to bring about a "mixed motives" and "bias towards the advertisers and away from the needs of the consumers", they rightly noted that such embedded biases are often difficult to detect, yet their impact on the market could be significant.[7] Having initially contemplated licensing their technology, Page and Bring spent considerable time exploring a viable business model, one that would uphold their values and address their genuine concern.[8] Observing the development of paid search advertising services like GoTo.com, they were ultimately presented with a pragmatic example of how search could be monetised: by essentially pioneering an auction-based pay-per-click model that would enable advertisers to bid for keyword positioning, the model ultimately turned search queries into commodified assets.[9] While economically effective and seemingly resistant to spam, the model nevertheless raised ethical concerns, as it mixed paid listings with organic results.[10] It was built as an "engine of purchasing intent" determined in accordance with the "accountable market valuation process"[11], offering a compelling commercial logic and a business sustainability promise. Despite the initial reluctance, however, Google ultimately followed suit in the aftermath of the dot.com crash, adopting the model and replicating its keyword-bidding system ("AdWords"), though with an intended and initially visible distinction that ensured the separation of sponsored content from organic search results.[12] It

---

[3] Gleason Archer, *Big Business and radio* (American Historical Company 1939)
[4] Ibid 64
[5] Ibid 65
[6] Wu (n 1) 77
[7] Sergey Brin and Lawrence Page, 'The Anatomy of a Large-Scale Hypertextual Web Search Engine' (Stanford University 1998) http://infolab.stanford.edu/~backrub/google.html accessed 31 August 2025.
[8] John Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (Portfolio 2005) 97, 108-109.
[9] Ibid, 109-112, 125-126
[10] Ibid, 131
[11] Ibid, 127, see also description in Darren J Davis, Matthew Derer, Johann Garcia, Larry Greco, Tod E Kurt, Thomas Kwong, Jonathan C Lee, Ka Luk Lee, Preston Pfarner and Steve Skovran, *System and method for influencing a position on a search result list generated by a computer network search engine* (US Patent US 6269361 B1, 31 July 2001)
[12] Battelle (n 8) 141. Case AT.39740 — Google Search (Shopping), Commission Decision C(2017) 4444 final, 27 June 2017; also Lucas D Introna and Helen Nissenbaum, 'Shaping the Web: Why the Politics of Search Engines Matters' (2000) 16(3) The Information Society 169; Federal Trade Commission, 'Letter to Search Engine Companies Regarding Disclosure of Paid Placement and Paid Inclusion' (27 June 2002) https://www.ftc.gov/sites/default/files/documents/closing_letters/commercial-alert-response-letter/commercialalertletter.pdf accessed 31 August 2025

originally introduced its first paid listings using a cost-per-impression (CPM) model, where advertisers were charged each time an ad was viewed, regardless of any possible user interaction.[13] The model was later replaced by a more performance-driven and quality-based weighting system: instead of ranking ads solely by the price of the bid, Google calculated ads' effective bid by multiplying the advertier's cost-per-click bid by a quality score, which was based among other things on a search ad's predicted click-through rate (CTR), derived from Google's proprietary predictive algorithm.[14]

Over time, this foundational for Google model evolved into a more complex auction mechanism, with distinct pricing levers such as squashing, which artificially boosts the runner-up's predicted CTR to increase competition; randomised generalised auctions (dGSP), which essentially swaps the top two bids to introduce uncertainty and encourage higer bidding; and format pricing, which ultimately increases the cost of ads with additional links or visuals.[15] This real-time bidding (RTB) is a core component of Google's adtech infrastructure that is grounded in pervasive tracking. Thus, bid requests are commonly enriched with granular user data, including IP addresses, device IDs, precise geolocation, browsing history, demographics, and inferred sensitive information. The data is then broadcast to hundreds of adtech actors within milliseconds of a page loading, enabling instantaneous and targeted advertising.[16]

The practice is increasingly being questioned both from a data protection perspective, focused on concerns around transparency, security, and lawful basis for data processing[17], but also from competition and consumer protection law viewpoints, where considerations center on the market power, exclusionary conduct, and barriers to entry.[18] What these ongoing probes and regulatory discussions reveal is the deep complexity and the intervowen nature of the ad tech infrastructure: real-time bidding is not an isolated set of processes. Rather, it is merely a component of the data-driven ad ecosystem where tracking feeds recommendation systems, which in turn optimise engagement for monetisable impressions, all of which are based on predictive algorithms trained on various signals largely deduced from behavioural data.[19] Depending on the business model and user interaction patterns, this infrastructure supports different types of advertising, each of which might express recommendation and engagement in a distinct manner. Thus, in search-based advertising, "recommendation" functions as a proxy for the expected usefulness of users' "intent", expressed, for instance, in ad relevance and ranking or in a feature of autocomplete[20] and "people also ask" attribute.[21] In social media and video platforms, on the other hand, recommendation systems appear more pronounced and somewhat autonomous, actively curating content feeds based on inferred interests, peer

[13] Benjamin Edelman and Thomas R Eisenmann, Google Inc. (Harvard Business School Case 910–036, 28 January 2010, rev April 2011) 3

[14] Case AT.39740 — Google Search (Shopping), 9.

[15] *United States of America et al v Google LLC; State of Colorado et al v Google LLC*, Memorandum Opinion, Nos 20-cv-3010 (APM) & 20-cv-3715 (APM) (D DC, 5 August 2024) para 238-246

[16] See more in Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23(2) *German Law Journal* 226

[17] e.g. Belgian Data Protection Authority (Litigation Chamber), *Decision on the merits 21/2022* (2 February 2022) DOS-2019-01377, 'Complaint relating to Transparency & Consent Framework (IAB Europe)'

[18] e.g. European Commission, 'AT.40670 — Google – Adtech' (Public case register) https://competition-cases.ec.europa.eu/cases/AT.40670

[19] e.g. discussions of the strength of the signal capturing consumer's purchase intent in (n 15), para 168-171, and 206-210 for a discussion on social media ads' signalling.

[20] Google, 'How Google autocomplete predictions work' (Google Search Help) https://support.google.com/websearch/answer/7368877?hl=en#zippy=%2Cwhere-autocomplete-predictions-come-from accessed 31 August 2025

[21] Markitors, 'What Is Google's "People Also Ask" Feature?' (Markitors) https://markitors.com/what-is-googles-people-also-ask-feature/?utm accessed 31 August 2025

activity, and registered interactions.[22] Likewise, "engagement" may be expressed and anchored differently across platforms: from links' clicks to likes, shares, or measured presence on a given page. All considered, however, even different interfaces and modes of used interaction cannot obscure the fact that various advertising formats across platforms are commonly perceived as complementary by marketing professionals and, from a functionality standpoint, are ultimately aligned around a shared logic of data-driven personalisation.[23] Whether through search, social interaction or video formats, the digital ad ecosystem deeply relies on a unified model of targeting and prediction, the model that has historically been presented as "free" access to digital services, where users' currency is manifested through their attention, behaviour, and personal data.

B. Subscription as a false exit

In this context, the subscription model presents itself as both a remedy and a means of reinforcement of the very dynamics it seeks to confront. On one side, it could be seen as a response to demonstrated inefficiencies of the ad-based ecosystem. As a growing body of scholarship has demonstrated, these inefficiencies emerge not only from established challenges in advertising measurement and accountability, but are also attributable to the structural design of the digital environment, which implies opacity, inscrutinasable intermediation, and fragmentation of users' digital experiences.[24]

Thus, one major issue lies in the difficulty and unreliability of measuring ad effect in digital advertising: despite the availability of a vast volume of often granular data, establishing a link between ad exposure and actual consumer behaviour remains a significant challenge. Several systemic and behavioural factors could explain such unreliability of digital advertising attribution models. For example, users' digital experiences unfolding across multiple devices and platforms pose a challenge to tracing a single ad's influence on a consumer outcome. Advertisers' own behaviour, such as targeting based on anticipated demand, could also introduce confounding variables that might skew attribution. Moreover, consumer behaviour itself is highly variable and context-dependent, complicating efforts to present a coherent causal interpretation of the ad effect.[25]

Another factor questioning the effectiveness of digital ads could be seen in organisational frictions and inefficiencies that the digital environment often amplifies. As the digital advertising supply chain includes a complex web of intermediation, where numerous adtech actors contribute to opacity and misaligned incentives, the actual ability of advertisers to maintain accountability over their budget allocation and spending is significantly undermined.[26]

Finally, the growing prevalence of ad blockers, while a clear manifestation of user's (dis)satisfaction with the prevalent model of ad delivery, also disrupts the financial viability of

[22] e.g. Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35(2) *Berkeley Technology Law Journal* 367

[23] e.g. a discussion on "funneling" in (n 15) para 72-76.

[24] Brett R Gordon and others, 'Inefficiencies in Digital Advertising Markets' (2021) 85(1) *Journal of Marketing* 7; Anshuman Sharma and others, 'Investigating the effect of advertising irritation on digital advertising effectiveness: A moderated mediation model' (2022) 180 *Technological Forecasting and Social Change* 121731.

[25] Supporting evidence in (n 24)

[26] e.g. Gordon (n 24) on a traditional issue of moral hazard; Yash Vekaria, Rishab Nithyanand and Zubair Shafiq, 'The inventory is dark and full of misinformation: Understanding ad inventory pooling in the ad-tech supply chain' in *Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP)* (IEEE 2024) 1590–1608 on fraud in a supply chain

the digital ad ecosystem.[27] By limiting ad exposure for users, they naturally reduce the effectiveness of monetisation strategies and risk undermining the publishers' incentives to invest in quality content, thus resulting in a potential net welfare decline.[28]

Taken together, these examples of the prevalent digital ad ecosystem both expose its structural vulnerability and multi-actor dependency and pose legitimate concerns over its overall impact on the integrity and quality of content production on the web at large. Against this background, a subscription model offers a potentially attractive alternative. Thus, for example, it has been shown that a subscription model, in principle, allows companies to build more direct and transparent relationships with users.[29] By moving from one-time transactions to recurring revenue streams, it also offers a more predictable income flow that allows for improved organisational planning.[30] However, while these attributes might mitigate some of the challenges related to, for example, opacity and measurement of the efficiency of the ad-based ecosystem, they do not eliminate or fully address the underlying incentives and logics governing digital platform economies.

One of the most enduring manifestations of this logic has been the emergence of a cultural and economic convention of "free" as the default mode of access.[31] As demonstrated, it has ultimately conditioned users to devalue web-available information as a product: users' expectations have come to define a "reference price of zero" for information access as both a cognitive attribute and an established market norm aligned with the notion of a "public good".[32] Thus, in transitioning from the status quo to a subscription model, platforms are challenged not only to justify and clearly explain the added value of the information behind the paywall but also to explore behavioural patterns that could help to instill a sense of its usefulness and thus reshape users' expectations.[33] Examples of possible strategies include the removal of ads across hosted videos and banner/search ads throughout the platform,[34] ad-free music listening,[35] third-party ads and trackers blocking,[36] improved functionality and premium features for coprorate clients[37] and bundled offering of a tracking protection, secure VPN access, and personal

---

[27] Gordon (n 24) 28-33

[28] Aleksandr Gritckevich, Zsolt Katona and Miklos Sarvary, 'Ad blocking' (2022) 68(6) *Management Science* 4703.

[29] Tony Chen, Ken Fenyo, Sylvia Yang and Jessica Zhang, *Thinking inside the subscription box: New research on e-commerce consumers* (McKinsey & Company, February 2018).

[30] Elie Ofek and Amy Konary, *'Subscription Models: Recurring Revenues for Lasting Growth'* (Harvard Business School Background Note 523-113, August 2023)

[31] e.g. Pew Research Center, *'Few Americans pay for news when they encounter paywalls'* (24 June 2025) https://www.pewresearch.org/short-reads/2025/06/24/few-americans-pay-for-news-when-they-encounter-pay-walls/ accessed 31 August 2025; Pinar Akman, 'A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets' (2022) 16(2) *Virginia Law & Business Review* 217

[32] Girish Punj, 'The relationship between consumer characteristics and willingness to pay for general online content: implications for content providers considering subscription-based business models' (2015) 26(2) *Marketing Letters* 175.

[33] Ibid; Liu Y, Park Y and Wang H, 'The mediating effect of user satisfaction and the moderated mediating effect of AI anxiety on the relationship between perceived usefulness and subscription payment intention' (2025) 84 *Journal of Retailing and Consumer Services* 104176; Adam Gabbatt, 'Value of X has fallen 71% since purchase by Musk and name change from Twitter' (The Guardian, 2 January 2024) https://www.theguardian.com/technology/2024/jan/02/x-twitter-stock-falls-elon-musk accessed 31 August 2025.

[34] Google, *'Use your YouTube Premium benefits',* https://support.google.com/youtub`ze/answer/6308116?hl=en accessed 31 August 2025

[35] Spotify, *'Premium',* https://www.spotify.com/dk-en/premium/ accessed 31 August 2025

[36] Brave, *'Brave Shields',* https://brave.com/shields/ accessed 31 August 2025

[37] OpenAI, *'ChatGPT Enterprise',* https://openai.com/index/introducing-chatgpt-enterprise/ accessed 31 August 2025

identifiers' removal services.[38] At the same time as behavioural recalibration is required from the user's perspective, the service provider is also confronted with an analytical shift that lies in structuring the corporate value proposition to secure recurring revenue.[39] In this paradigm, data and personalisation become more like an operational core rather than a secondary consideration: behavioural signals not only act as a means of shaping users' habits and optimising their retention, they can also play a decisive role in guiding content decisions, embedding real-time users' preferences into creative processes.[40] Thus, rather than heralding a departure from a data-dependent infrastructure, the subscription model reconfigures that reliance. While seemingly moving away from the pervasive targeting practices of the ad-funded environment, it nevertheless continues to utilise data as a key operational asset to support customer retention, service calibration, and user-driven content optimisation.[41]

This dynamic is particularly pronounced in the development of Meta's "ad-free" subscription model, which emerged as a response of the sustained regulatory pressure on the one hand, and keeps evolving in the face of multiple, still ongoing, investigations in the company's data practices on the other. The initial version of the model, often referred to as "pay-or-consent" or "Pay or OK", was introduced in November 2023, and offered users a binary choice of either consenting to behavioural tracking for personalised advertising or paying a monthly subscription fee to use the platform without ads. In its public announcement, the model was claimed to "balance the requirements of European regulators while giving users meaningful choices over how their data is used," in response to several "evolving and emerging regulatory requirements".[42]

C. Consent or pay

This framing, however, needs to be situated within the broader regulatory trajectory that preceded it. In December 2022, the EDPB adopted a Binding decision establishing that Meta could not lawfully rely on contractual necessity as a ground for data processing for advertising purposes, as the latter is not "objectively necessary to deliver the service and is not an essential or core element of it".[43] The EDPB position was further affirmed by the CJEU ruling in *Bundeskartellamt v Meta* case delivered in July 2023.[44] In its judgement, the Court underscored that Meta's business model fundamentally hinges on a technical ad-driven infrastructure that enables the systematic collection of a variety of user- and device-related data, both on and off the platform, for the purpose of creating detailed user profiles.[45] The Court then clarified that

---

[38] DuckDuckGo, *'DuckDuckGo Subscription (non-U.S.) Privacy Policy and Terms of Service',* https://duckduckgo.com/pro/privacy-terms/non-us/en accessed 31 August 2025

[39] Christoffer Weland Johannes Lindström, Behzad Maleki Vishkaei and Pietro De Giovanni, 'Subscription-based business models in the context of tech firms: theory and applications' (2024) 6(3) *International Journal of Industrial Engineering and Operations Management* 256

[40] Ibid; but also Tim Groot Kormelink, 'Why people don't pay for news: A qualitative study' (2023) 24(10) *Journalism* 2213;
but also Helle Sjøvaag, *The markets for news: enduring structures in the age of business model disruptions* (Routledge 2022)

[41] Lindström (n 39)

[42] Meta, *'Facebook and Instagram to Offer Subscription for No Ads in Europe'* (12 November 2024) https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe accessed 31 August 2025

[43] European Data Protection Board, *'Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art 65 GDPR)'* (5 December 2022), para 52 on submissions of DPAs and para 136 on the EDPB conclusion

[44] Case C-252/21 *Meta Platforms and Others v Bundeskartellamt* EU:C:2023:537

[45] (n 44), paras 27, 52

for such data processing to be grounded in contractual necessity under Article 6(1)(b), it must be objectively indispensable for fulfilling a purpose that is intrinsic to the contract itself.[46] In other words, it should be beyond doubt that the core functionality of Meta's social networking service could not be delivered without behavioural tracking and subsequent profiling. Furthermore, there must be no less intrusive and equally effective alternative available, capable of justifying the choice of contractual necessity as a lawful basis.[47] As the Court acknowledged, however, even though personalisation may be useful to users in a way that it allows them to view content aligned with their interests, it does not satisfy the threshold of necessity. The services of the social network can, in principle, be provided in the form of an "equivalent," non-personalised alternative.[48]

The CJEU then examined Meta's reliance on "legitimate interest" under 6(1)(f) as a ground for data processing. As the Court emphasised, data processing in this case is only lawful when and if three cumulative conditions are met. First, the controller must pursue a legitimate interest related to its economic and commercial activity, which is clearly communicated to data subjects.[49] Second, the processing must be strictly necessary for achieving that interest, interpreted narrowly and in conjunction with the "data minismisation" principle under Article 5(1)(c).[50]Third, the legitimate interest must not be overridden by the fundamental rights and freedoms of the data subject, which requires balancing of interests on a case-by-case basis.[51]

In assessing the applicability of legitimate interest under Article 6(1)(f), the Court reviewed several potential justifications mentioned by the referring court, such as personalised advertising, network security, and product improvement. While examining these possible legitimate interests, the Court underscored several overarching and all-embracing considerations, largely reiterating the long-standing practice of considering the balancing between the controller's interests and fundamental rights and freedoms of data subjects.[52]Thus, the CJEU stressed the importance of taking into account the reasonable expectations of data subjects, as well as the scale and impact of data processing.[53] It emphasised a strong connection between consent and reasonable expectations: even if the service was offered free of charge, the absence of data subjects' consent, in the eyes of the Court, undermined any assumption that individuals should, or could have expected, that their data would be used for advertising.[54] The CJEU also pointed out that the extensive scope of data processing at issue, involving "potentially unlimited data", has a significant impact on data subjects and may also create the impression that their life is being continuously monitored.[55] The language of the decision largely echoes earlier findings and conclusions of both the Court and the Advocate General in the 2014 Digital Rights Ireland case, where it was observed that the retention and use of data without the data subjects' knowledge is likely to give rise to a feeling of constant surveillance.[56] While the practices largely differ in both main actors and aims, it is striking that both cases

[46] (n 44), para 98
[47] (n 44), para 99
[48] (n 44), para 102
[49] (n 44), paras 106, 107, 124.
[50] (n 44), paras 108-109
[51] (n 44), paras 110-111
[52] Article 29 Data Protection Working Party, *'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'* WP 217 (9 April 2014)
[53] (n 44), paras 112, 116, 118, 123
[54] (n 44), para 117
[55] (n 44), 118.
[56] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* EU:C:2014:238, para 37. Opinion of AG Cruz Villalón in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* EU:C:2013:845, delivered on 12 December 2013, paras 52 and 72.

fundamentally raise similar questions about the limits of data processing and the risk of normalising pervasive surveillance, whether state-driven or commercially motivated.

The CJEU then proceeded to examine the issue of consent guided by the enquiry of the referring court and specifically addressing the implications of the stated dominant position of the platform on the market for online social networks. As the Court acknowledged, the finding of dominance in itself does not invalidate consent.[57] However, it must be factored into assessing whether consent is freely given, particularly if refusing consent results in exclusion from the core services.[58] Against this background, the Court sets forth the requirement that users must retain the ability to refuse, on an individual basis and within the contractual process, consent to specific data processing operations that are not strictly necessary for the provision of the service. In such cases, users cannot be compelled to forgo access to the service altogether. Rather, they must be offered, "if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations."[59]

Following the CJEU deliberations in the *Bundeskartellamt v Meta case*,[60] the EDPB was presented with the request from the Norwegian Data Protection Authority to take urgent action under Article 66(2).[61] The request was grounded in Meta's continued processing of personal data for behavioural advertising based on alleged contractual necessity and legitimate interests of the platform. Having established that these practices essentially amounted to Meta's ongoing infringement and posed significant risks to data subjects' rights and freedoms, EDPB concluded that final measures were appropriate, proportionate, and necessary, ultimately ordering a ban on such processing across the entire EEA[62]. The timing of these enforcement actions coincided with the effective introduction of new obligations under the Digital Markets Act (DMA), particularly Article 5(2), which Meta was required to comply with following its designation as a gatekeeper.[63]

It was in this context that Meta rolled out its "consent or pay" subscription model in early November of 2023 as a compliance response.[64] Simultaneously, it also "temporarily" suspended all advertising to users under 18 in the EU, EEA, and Switzerland.[65]

The developments prompted regulatory engagement on a variety of fronts. On January 17, 2024 the Dutch data protection authority, acting also on behalf of the Norwegian and German (Hamburg) supervisory authorities, submitted a request to the EDPB pursuant to Article 64(2). The referral concerned the circumstances under which "consent or pay" models can be considered compatible with the definition of consent as stipulated in the GDPR and developed in the relevant decisional practice. While acknowledging that some national regulators had issued guidance on "consent or pay" at the national level, typically in specific contexts and often in relation to smaller controllers, the requesting authorities stressed the need

[57](n 44), paras 147, 154
[58] (n 44) para 148
[59] (n 44) para 150
[60] *Case C-252/21 Meta Platforms Inc and Others v Bundeskartellamt* EU:C:2023:537 (CJEU, 4 July 2023)
[61] European Data Protection Board, *'Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art 66(2) GDPR)'* (27 October 2023)
[62] Ibid, paras 314-325
[63] 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 (Digital Markets Act) [2022] OJ L 265/1, art 5(2).
[64] See, e.g. European Data Protection Board, 'Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art 66(2) GDPR)' (27 October 2023), para 110, European Commission, Case DMA.100055 – Meta – Article 5(2) (Decision under Arts 29(1), 30(1) and 31(1) Regulation (EU) 2022/1925, 23 April 2025), paras 9-16, 120.
[65] Meta Platforms, 'How do I manage my information on Messenger?' (Facebook Help Centre) https://www.facebook.com/help/messenger-app/229435355723442/ accessed 31 August 2025

for a harmonised approach capable of ensuring a consistent interpretation in cases involving large online platforms[66].

The issued EDPB Opinion largely accommodated these focal points by explicitly delimiting the scope of its assessment to subscription models in which data subjects are allowed to access a version of the service that excludes the processing of the users' personal data for behavioural advertising, in exchange for a fee.[67] The subscription models under consideration are implemented by controllers of "large online platforms", which attract a large amount of users in the EEA and engage in large-scale data processing. The category may encompass, but is not limited to "online platforms" under article 3(i) of the Digital Services Act, and may also include designated "very large online platforms" under the DSA and "gatekeepers" under the Digital Markets Act.[68]

The EDPB's Opinion largely builds upon and reiterates established practice in assessing consent,[69] while also attempting to nuance its application in the context of large online platforms, particularly in light of the Court's *Bundeskartellamt decision* and the DMA requirements. The Opinion addresses the concept of an "equivalent alternative". It unequivocally rejects the notion that such an alternative could be satisfied by a service offered by another controller, stressing that freedom of choice cannot be externalised or made contingent upon market dynamics.[70] Equivalence, in this context, is not merely formal; it is essentially about maintaining a comparable user experience.[71] Thus, an alternative version may be deemed equivalent if it retains the same essential features, functionality, and service quality, subject only to changes that are strictly necessary due to the absence of extensive personal data processing.[72]

As the EDPB also makes clear, offering only a paid alternative to consent for behavioural advertising should not be the default approach.[73] Instead, controllers are encouraged to provide a version of the service that does not involve tracking-based advertising and may rely on less intrusive forms, such as contextual or topic-based ads.[74] In this context, the proposed "Free Alternative Without Behavioural Advertising model" seems to function as both a normative benchmark and a practical safeguard in shaping the EDPB's analysis of valid consent. The EDPB repeatedly refers to this model as a strong indicator that consent has been freely given, viewing it as evidence that the controller has made efforts to mitigate the risks of coercion, conditionality, and power imbalance.[75] As such, it may be understood as a proposed functional

[66] European Data Protection Board, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' (17 April 2024) para 6; Importantly, there is also a number of case decisions at the national level considering "consent or pay" in different contexts, see, e.g. Personvernnemnda (Norwegian Privacy Appeals Board), *PVN-2022-22 Grindr – disclosure of personal data without valid consent – administrative fine* (27 September 2023); Commission nationale de l'informatique et des libertés (CNIL), 'Cookie walls: the CNIL publishes the first evaluation criteria' (16 May 2022); Digitaliseringsstyrelsen and Datatilsynet, *Brug af cookies og lignende teknologier: Vejledning* (May 2025); as well as a recent decision on pay or consent in Austria, see Bundesverwaltungsgericht (Austria), *W291 2272970-1/30E, W291 2272971-1/32E* (18 August 2025) — case note available at GDPRhub, https://noyb.eu/sites/default/files/2025-08/20250818145608738p_Redacted.pdf accessed 31 August 2025

[67] European Data Protection Board (n 66) para 14-16

[68] European Data Protection Board (n 66) paras 23-28

[69] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (4 May 2020)

[70] European Data Protection Board (n 66), para 120

[71] European Data Protection Board (n 66), para 123

[72] European Data Protection Board (n 66), paras 121-126.

[73] European Data Protection Board (n 66), para 73

[74] European Data Protection Board (n 66), paras 73-76

[75] European Data Protection Board (n 66), paras 73, 74, 77, 79, 80, 87, 117, 127.

mechanism to guide regulatory enforcement: where no such option is offered, the validity of the consent may be called into question.[76]

Finally, the EDPB, following the Bundeskartellamt decision, acknowledges that if a fee is imposed on users who do not consent to behavioural advertising, such a fee must be fair, proportionate, and must not exert pressure on users to consent.[77] The EDPB emphasises that personal data cannot be treated as a tradable commodity: the right to data protection, as enshrined in Article 8 of the Charter of Fundamental Rights, is a fundamental right, not reducible to a transactional privilege.[78]

The EDPB Opinion was challenged by Meta in proceedings before the General Court, combining an action for annulment with a claim for damages.[79] Meta advanced a series of pleas contesting both the substance of the Opinion as well as the procedure by which it was adopted. It argued that the Opinion unlawfully constrained its business model and introduced expansive obligations beyond the GDPR, thereby upsetting the balance between its freedom to conduct business and data protection rights. The General Court dismissed the action, holding that the EDPB Opinion lacks a binding effect and thus was not an act open to challenge under Article 263 TFEU. The Court also stated that the Opinion was advisory in nature, did not alter Meta's legal position, and could only gain a binding force through subsequent decisions by supervisory authorities.[80]

In parallel with the ongoing scrutiny of the model under data protection law, a separate but closely related assessment of the model was initiated under the DMA. According to Article 5(2) of the DMA, gatekeepers are prohibited from processing, combining, or cross-using data across core platform services and other services unless the end user has been presented with a specific choice and has given consent within the meaning of Article 4 and Article 7 of the GDPR.[81] The provision, in principle, is meant to serve a core regulatory objective of preventing gatekeepers from exploiting their position to aggregate personal data across services, thereby raising barriers to entry.[82] As clarified in Recital 36 and 37 of the DMA, the right to refuse such data processing must be meaningful and effective in requiring that gatekeepers, in their turn, offer a "a less personalised but equivalent alternative" that does not condition access to the core service on consent. It further clarifies that the "less personalised alternative" should not differ in substance or quality from the service offered to users who provide consent, except where any degradation of quality results from the gatekeeper's inability to process personal data or sign end users into the service.

It was against this regulatory backdrop that the Commission launched its formal investigation into Meta's 2023 "consent or pay" model, shortly after the company submitted its compliance report in March 2024, describing the measures it had implemented to meet its obligations, including the introduction of the subscription option as a primary mechanism for satisfying the requirements of Art. 5(2) DMA.[83] As the Commission established in its decision of April 23, 2025, Meta failed to comply with the requirements of Article 5(2) in two key respects. First, it did not present users with the specific choice to combine or not their personal data across its services, in particular with regard to its non-ad services (such as Facebook and

[76] European Data Protection Board (n 66), paras 179, 181.
[77] European Data Protection Board (n 66), para 134
[78] European Data Protection Board (n 66), para 130, 132.
[79] *Case T-319/24 Meta Platforms Ireland Ltd v European Data Protection Board* EU:T:2025:435 (General Court, 29 April 2025)
[80] Ibid, para 29
[81] Digital Markets Act, Rec.36
[82] Wolfgang Kerber and Louisa Specht-Riemenschneider, *Synergies between Data Protection Law and Competition Law* (Verbraucherzentrale Bundesverband e.V., 30 September 2021) 72
[83] Case DMA.100055 – Meta – Article 5(2), para 16

Instagram) and its advertising service, Meta ads.[84] Second, the consent collected from users who opted for the ad-supported version of the service could not be considered valid under the standards of the GDPR, as defined in Articles 4 and 7. Importantly, the assessment was carried out from the perspective of the user experience within the Facebook and Instagram environments, rather than at the level of each individual service.[85] As a result, the Commission concluded that Meta had failed to offer a "less personalised but equivalent alternative".[86]

Alongside enforcement actions under competition law, the GDPR, and the DMA, Meta's market behaviour also became a subject of a consumer protection investigation under the EU Unfair Commercial Practice Directive (UCPD) and the Unfair Contract Terms Directive (UCTD). Thus, in November 2023, the European Consumer Organisation (BEUC) filed a complaint before the Consumer Protection Cooperation (CPC Network), arguing that Meta's subscription model amounted to both aggressive and misleading commercial practices.[87] BEUC essentially argued that the design of subscription choices exerted undue pressure on users, constituting an aggressive tactic prohibited under Article 8 UCPD. Furthermore, it contended that Meta's framing of "free" vs "paid" access risked misleading consumers, particularly by obscuring the fact that allegedly "free" access was conditional on the extensive processing of personal data. The CPC Network, led by the French consumer authority and coordinated by the EU Commission, opened a formal investigation into the matter.[88] Although Meta introduced limited adjustments to its pay-or-consent interface as a response, both BEUC and national authorities indicated that these changes did not fully address the original concerns around undue pressure and misleading commercial practices.[89]

D. Symptomatic enforcement

Following the evolution of advertising and subscription models from early examples of radio broadcasting to ad-supported Google services and more recent Meta's "consent or pay" subscription option, it becomes evident that monetisation grounded in user attention is not an isolated development or merely a novel business model strategy but rather is an expression of a deeper structural logic. Viewed holistically, regulatory responses often present the problem of adtech in terms of constrained choice and unlawful consent, framing it around the various available mechanisms designed to empower users as individual decision-makers, rather than confronting the deeper architectural conditions that sustain this imbalance in the first place. This seems to be largely because enforcement is multifaceted and fragmented, with the entry point into the regulatory process conceived through, for example, data protection, competition,

[84] Case DMA.100055 – Meta – Article 5(2), para 84
[85] Case DMA.100055 – Meta – Article 5(2), para 86
[86] Appealed by Meta: *Meta Platforms v Commission* (Case T-435/25), [2025] OJ C/2025/5214. At the time of writing, Meta's commitment to introduce a revised advertising choice model for EU users has been publicly acknowledged, but the specifc details of the EU implementation are not yet fully clear on the public record.
[87] BEUC, *'Consumer groups file complaint against Meta's unfair "pay or consent" model'* (BEUC Press Release, 30 November 2023) https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model accessed 31 August 2025
[88] European Commission, *'Consumer authorities to step up enforcement against illegal rip-offs by platforms'* (IP/24/3862, 6 June 2024) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3862 accessed 31 August 2025
[89] BEUC, *'Consumer groups red card Meta's latest pay-or-consent policy'* (BEUC Press Release, 22 January 2025) https://www.beuc.eu/press-releases/consumer-groups-red-card-metas-latest-pay-or-consent-policy accessed 31 August 2025, see also BEUC, *Meta's Latest Pay-or-Consent Policy: Analysis & Recommendations* (BEUC, January 2025) https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-002_Meta_s_latest_pay-or-consent_policy.pdf accessed 31 August 2025

or consumer rights often shaping not only the framing of the harm but also the scope of the remedy itself.

Thus, from the perspective of data protection law, the regulatory focus is heavily grounded in the notion of individual rights and lawful grounds for data processing. It assumes that individuals should have control over their personal data,[90] and that any interference with this control is possible only if certain normative thresholds, such as, for example, consent, contractual necessity, or legitimate interest[91], are met along with the overarching principles of data protection.[92] This regulatory orientation, as has been argued, can be understood through a distinctly individualistic lens, where individuals are expected to "adjudicate between legitimate and illegitimate information production," harm is primarily conceptualised in individual-affecting terms, and data governance is, by and large, premised on individual ordering as the default condition.[93]

Under this framing, legal tools like consent are construed to empower individuals to decide what forms of "information production" they prefer. However, the object of such production, personal data, is "non-rivalrous, non-extinguishable, reusable,"[94] and, by its very nature, relational.[95] Its circulation is mediated through complex technical infrastructures designed to optimise revenue extraction and enable continuous data repurposing.[96] Thus, a mere premise that individuals can meaningfully govern this process through the act of an on-off consent is misaligned with the structural realities of the data processing ecosystem. Furthermore, the narrow approach to constructing "harm" is also inadequate. Large online networks derive value not only from processing individual data points but from tracing connections, making inferences, and running affinity profiling practices across their entire ecosystem.[97] Thus, framing harm as "individual"-centered does not capture the damage potentially inflicted on societal and relational connections of data subjects.

In this context, examination of consent or pay model through the vocabulary and logic of data protection law often falls short. The EDPB, in attempting to confront the challenge of services funded through behavioural advertising, is adapting its interpretative apparatus to address impacts that are more structural than individual-centered. It weaves economic reasoning into a legal framework that was not originally built to accommodate and handle these systemic challenges consistently.[98] In doing so, the EDPB stretches the normative language, particularly concepts like individual autonomy, fairness, and freely given consent, by embedding assumptions about structural market asymmetries and advancing generalised expectations that go beyond case-specific logic per se.

---

[90] Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) [2016] OJ L119/1, Rec.7

[91] GDPR, Art. 6 and Art. 9

[92] GDPR, Art. 5

[93] Salomé Viljoen, 'A Relational Theory of Data Governance' (2020) 131 *Yale Law Journal* 573, 582, 594, 627.

[94] Ibid, 598

[95] danah m boyd and Nicole B Ellison, 'Social Network Sites: Definition, History, and Scholarship' (2007) 13(1) *Journal of Computer-Mediated Communication* 210, 211; Kevin Lewis and others, 'Tastes, Ties, and Time: A New Social Network Dataset Using Facebook.com' (2008) 30(1) *Social Networks* 330; Johan Ugander *et al.*, 'The Anatomy of the Facebook Social Graph' (2011) arXiv:1111.4503; Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880 1881;

[96] Case DMA.100055 – Meta – Article 5(2), para 5

[97] Scott Morton FM and Dinielli DC, *Roadmap for an Antitrust Case against Facebook* (Omidyar Network, June 2020), 4-5, Viljoen (n 93), Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35(2) *Berkeley Technology Law Journal* 369.

[98] This is not to disregard, however, the extensive bodu of literature that has sought to integrate both antitrust and data protection law pframeworks in assessment of market power. See, e.g. Costa-Cabral F and Lynskey O, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54(1) *Common Market Law Review* 11–50.

Thus, the attempt to offer a solution in the form of "Free Alternative Without Behavioural Advertising model", while normatively compelling, is structurally difficult to substantiate. Essentially, the EDPB appears to be advancing a kind of "safe harbour" compliance strategy, predicated on the implied recognition of an inherently clear imbalance of power presented by the complex and non-transparent architecture of platforms.[99] From the EDPB's viewpoint, consent then cannot then be used but for "exceptional circumstances" and where the controller can prove the absence of "adverse consequences at all" for the data subject if they do not consent. The proposition draws on Recital 43 GDPR, as elaborated in the EDPB Guidelines on consent, where the employment context is presented as a paradigm case of structural power imbalance.[100] The choice of an example is in itself interesting. While employment typically involves a formalised and institutionalised power imbalance, with a clear risk of coercion and significant consequences such as job loss and discrimination, the power asymmetry of social networks is more diffused and less formally structured. In drawing this with the employment context, however, the EDPB characterises the social network largely through the references to well-established economic attributes of network effects and switching costs.

In economics, both switching costs and network effects are often framed in terms of compatibility.[101] They are said to occur when consumers prefer a kind of compatibility that requires otherwise separate purchases to be made from the same firm. Switching costs arise when a consumer values compatibility across their purchases. This preference might stem from a reluctance to learn or adapt to new alternatives, or from the prohibitive costs of abandoning previous investments such as follow-on products, custom settings, or extended warranties tied to the original supplier.[102] At the same time, network effects occur when users value compatibility with other consumers. They may value it because it enhances the utility of consumption as more users join the network or because it grants access to a broader market of complementary goods.[103]

The EDPB translates these economic drivers into an acknowledgement that platforms with large user bases and embedded social functionality can create conditions where opting out becomes an unrealistic and practically infeasible option. As the EDPB notes, in this case, users are to sacrifice years of interaction, content creation, and employment prospects. In such settings, refusal to consent ultimately entails the loss of not only functional access, but also a form of meaningful participation in social, professional, or public life.[104] The reasoning behind bears a striking resemblance to the essential facility doctrine in competition law, which addresses scenarios where a dominant firm controls access to infrastructure so critical that denial of access to it without objective justification merits a principal antitrust scrutiny.[105] The difference, however, lies in the fact that the essential facility doctrine largely hinges on a combination of the facts of dominance and indispensability, requirements that are not really native to the data protection realm. In the EDPB analysis, these attributes are effectively presumed rather than substantiated through the formal enquiry. Even though this presumption

[99] GDPR, Rec.42

[100] Case DMA.100055 – Meta – Article 5(2), para 79, with the reference to EDPB Guidelines (n 69) para 22 and Example 5.

[101] Joseph Farrell and Paul Klemperer, 'Coordination and Lock-In: Competition with Switching Costs and Network Effects' in Mark Armstrong and Robert H Porter (eds), *Handbook of Industrial Organization*, vol 3 (Elsevier 2007) 1971.

[102] Ibid, 1972.

[103] see generally Michael L Katz and Carl Shapiro, 'Network Externalities, Competition, and Compatibility' (1985) 75 *American Economic Review* 424.

[104] European Data Protection Board (n 66) paras 88-89, 91-92, 109-110, 113

[105] See, e.g. Damien Geradin, 'Limiting the Scope of Article 82 EC: What Can the EU Learn from the US Supreme Court's Judgment in *Trinko* in the Wake of *Microsoft*, *IMS*, and *Deutsche Telekom*?' (2004) 41 *Common Market Law Review* 1519.

comes across as an intuitive and commonsensical finding, it risks lacking the necessary analytical depth and grounding to withstand the critique from the companies arguing that such a stance towards adtech significantly constrains their freedom to conduct business.[106]

In light of a "Free Alternative Without Behavioural Advertising model", the subscription-based model raises a set of further concerns. First of all, if the failure to provide a genuine free, ad-free alternative is framed as a possibly unjustifiable exclusion, it becomes difficult to reconcile how a subscription-based model, regardless of pricing, could meet the requirements of freely given consent.[107] In this paradigm, pricing in itself might be seen as an exclusionary threshold, especially, as discussed above in *Section B*, in cases where services of the platform have been historically available at zero monetary costs.[108] Clarifying the CJEU position in Bundeskartellamt, the EDPB offers little substantive elaboration on what constitutes an "appropriate fee" for the service. Instead, it refers to a need for a case-by-case assessment and conformity with data protection principles and the objectives of the GDPR in defining such a fee.[109] However, it remains unclear how data controllers are expected to interpret and operationalise such guidance in practice. The EDPB's reference to "fairness" as the guiding standard for setting an "appropriate fee" hardly provides any meaningful direction, as fairness is inherently contextual, and especially when it is applied to the circumstances of "the given case", as the Opinion requires.[110]

Given the conceptual framing and practical challenges of fee assessment within the Meta subscription model, the "pay or consent" option seems to be raising a more fundamental question: can the imposition of any fee be a feasible alternative? The question is especially challenging in light of economic forces and users' preferences discussed in *Section B*. As highlighted, in moving from an ad-funded model to a subscription-based one, companies are generally expected to justify and articulate the added value of the paid service to attract and retain customers. However, given the repeated regulatory references to the desirability of a "free alternative without behavioural advertisement" in lieu of the paid service, formulating the added value of the latter becomes particularly difficult. Thinking of possible user segmentation, one might propose that a "free" ad-funded model could appeal to those who, due to habit, convenience, or perhaps a genuine preference for detailed ad targeting and content calibration, might actively opt for target experiences. The user groups that might be choosing the "Free Alternative Without Behavioural Advertising model" or subscription model are, however, difficult to distinguish. Thus, both options are designed to eliminate or reduce behavioural advertising, as seen from the user's perspective, yet the functional and structural difference between the two remains elusive. While potentially employing some procedural restrictions, possibly in different forms, on third-party involvement for ad targeting purposes, they are unlikely to have a long-lasting effect on the platform's own data collection practices. It seems that core data gathering for purposes such as service optimisation or user engagement, or general content ranking, and internal analytics remains, by and large, intact.

Moreover, they may not even achieve their intended effect. Since data, as highlighted in *Section D*, is inherently relational and shaped collectively, through social ties, network connections, and networked behaviour, it may be proposed that as long as a critical mass of users continue to operate within the ad-subsidised model, the preferences, behaviour, and connections of those who have opted out of behavioural ads may still be inferred. As general content ranking and internal analytics seem to be largely unaffected across both models, continued profiling and optimisation appear to be able to sustain themselves based on

[106] e.g. Case DMA.100055 – Meta – Article 5(2), para 119, 146
[107] see, e.g. Case DMA.100055 – Meta – Article 5(2), para 132
[108] Case DMA.100055 – Meta – Article 5(2), para 109
[109] Case DMA.100055 – Meta – Article 5(2), paras 85, 133
[110] Case DMA.100055 – Meta – Article 5(2), para 135

aggregated user activity. This regulatory spillover effect seems to be effectively undermining the premise of meaningful content-driven privacy segmentation and highlights the natural limits of the "individual right"-based perspective.

E. Architecture of choice and choice of architecture

Against this background, a regulatory response accommodating market drivers and structural logic seems to be a naturally more appropriate entry point, one that shifts the attention from the individualistic conception of a data subject as an adjudicator of "information production" towards a more principal recognition of how platforms' architectural choices and structural incentives shape user behavior. The implications of digital business models for competition law and policy, particularly in relation to data as a barrier to entry and a driver of the network effects, have long been a key focus of several reports commissioned and produced at various regulatory and governmental levels.[111] In this context, the conventional antitrust path of scrutinising market conditions and the effect of "data power" has drawn both strong support as well as substantive criticism.[112] Divergent national practices and approaches to the application of competition law have further contributed to and deepened what has been described as an "identity crisis" in the field.[113] In effect, the regulatory model of the DMA could be seen then as a step towards the post-crisis rebuilding aimed at the integration of both collective and individual-centered considerations in assessing the role and positioning of platforms on the market.[114] Thus, the DMA explicitly recognises that the data protection and privacy interests of end users are relevant to evaluating the potential harms associated with gatekeepers' practice of collecting large amounts of data from users.[115]

The undeniably intended complementarity of the DMA and the GDPR can be traced and broadly characterised as normative complementarity, seen through shared objectives and protected values;[116] operational complementarity expressed in common mechanisms, definitions, and concepts,[117] and enforcement complementarity advanced through the cooperation and expected synergy in implementing and supervising compliance.[118] Taken together, these dimensions suggest a deliberate space for cross-fertilisation between more individual-centered and

---

[111] e.g. Autorité de la concurrence and Bundeskartellamt, 'Competition Law and Data' (10 May 2016) (Joint paper); Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era' (Report for the European Commission, 2019); OECD, 'Consumer Data Rights and Competition—Background note' DAF/COMP(2020)1 (29 April 2020).

[112] e.g. James C Cooper, 'Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity' (2013) 20 *George Mason Law Review* 1129, Maureen K Ohlhausen and Alexander P Okuliar, 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) 80 *Antitrust Law Journal* 121; Orla Lynskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 *Theoretical Inquiries in Law* 189; Anne C Witt, 'Excessive Data Collection as Anticompetitive Conduct: The German Facebook Case' (2020) Jean Monnet Working Paper 01/20

[113] eee, e.g. a discussion in Malte Frank and Emma Grace Lewis, 'The European Commission's Challenge to Consent or Pay: Demystifying the Digital Markets Act?' (2024) 47 World Competition 427

[114] However, see, e.g. Nicolas Petit, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review' (2021) 12 *Journal of European Competition Law & Practice* 529 for a discussion on the DMA projected objectives

[115] Digital Markets Act, Rec.72

[116] e.g. cf DMA Rec.4, 33, 62 on the language of empowerment and renegotiating the power imbalance, Rec. 70 on user autonomy and e.g. fairness as a principle of the GDPR (Art.5, Rec. 39, 60)

[117] See more and a nuanced discusison in a recent draft European Data Protection Board and European Commission, *Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation* (version for public consultation, 9 October 2025).

[118] e.g. European Data Protection Supervisor, *Opinion 2/2021 on the Proposal for a Digital Markets Act* (10 February 2021)

more structurally oriented regulatory approaches.[119] This shared space could be seen as marking a shift from an isolated and distinct regulatory logic to a coordinated governance architecture. However, when it comes to social networks, the effective enforcement requires more than the pragmatic and inconsistent use of tools and terminology borrowed from various regulatory regimes governed by distinct logic. It calls for a network-aware framework that accounts for users' structural dependencies within the digital infrastructure. In essence, it demands acting within and on the network logic.

Regardless of whether user segmentation is implemented through a "free-tier" and paying subscribers or through the introduction of a "free alternative without behavioural advertisement" model, users' experience and data processing patterns remain inherently guided by the network dynamics. In other words, even paying users continue to function as nodes within a broader network that typically has connections, flows, and relational dynamics in its structure.[120]

In this context, the DMA has the potential to instituionalise the network-level intervention. By constraining, for example, cross-device data combination and cross-use, prohibiting certain self-preferencing patterns, reinforcing end-user data portability, and supporting interoperability, where applicable, it attempts to rewire connections, weaken the effect of user lock-in, and constrain leveraging of social-graph inferences.[121] Thus, the DMA exemplifies, in essence, the idea of the network-centrality-based regulation, targeting, for example, structural nodes ("gatekeepers") and trying, to some extent, open network boundaries through interoperability mandates.

However, grounding some of these regulatory endeavours within traditional mechanisms of data protection rules, such as consent, presupposes that expressions of individual autonomy and agency, encapsulated in a transactional nature of consent, could be meaningfully disentangled from collective effects created by the embeddedness of users in a structurally relational system of a social network. This assumption, though, is fundamentally challenged by the very functioning logics and revenue sources of the platforms themselves. Core network dimensions, such as, for example, the social graph or identity layer, are inextricably linked to the revenue model, be that entirely ad-based or subscription-based paradigm. In figures of data protection, these individual choices, made at scale, effectively form the normative baseline of reasonable expectations of privacy and data protection for all. It follows, users' autonomy, while central to the regulatory architecture, is often exercised within structurally constrained conditions. These very architectural constraints, then, in turn, come to define and capture the dominant expectation of protection.

Recognising this dynamic invites a more thorough discussion on how to better align the DMA network-level intervention with the foundational values of data protection, such as respect for human dignity and users' autonomy, without allowing the architecture to undermine or unjustifiably reshape users' expectations of privacy and data protection. One way to achieve it could be through consistently recognising this power of architecture and intentionally leveraging it to advance data protection values. Thus, despite the DMA's focus on structural nodes and network boundaries, it largely overlooks the value of one's identity, along with social graphs, and the relational nature of harm on the network. In many ways, these concepts capture core aspects of and largely relate to individual dignity and autonomy while also acting as structural enablers of gatekeepers. To better acknowledge their enabling faculty, these concepts

[119] see, e.g. Inge Graef and Sean van Berlo, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility' (2021) 12 *European Journal of Risk Regulation* 674

[120] Manuel Castells, *The Rise of the Network Society* (Blackwell 1996)

[121] E.g., DMA Art 5(2), Art 6(5), 6(9), Art 7, with an additional caveat that Art 7 could be extended beyond NIICS, to cover online social networking services at large (Art.53).

could have been more explicitly recognised within the DMA, specifically under categories such as, for instance, a *network control layer* (capturing data flows), *infrastructural assets* (such as identity and social graphs), and a *network-sensitive theory of harm* (accounting for relational harm as a collective risk factor).

Such a conceptual revision could have had a meaningful impact on existing DMA requirements under, for example, data access, data portability, and performance measurement requirements.[122] In particular, the DMA could have specified more clearly that compliance requires not only access to relevant data streams as such but also access to the interfaces and operational parameters necessary to make this access effective in practice. Thus, to render the network layer observable, gatekeepers could have been required to provide, along with relevant datasets, a set of specifications needed to interpret and check these datasets. This could include, for example, adopted definitions and measurable outcomes (e.g., what exactly is captured by 'impression,' 'active user' or 'interaction' in the relevant context) and information as to how the data is generated and recorded (e.g., whether it originates from users' devices or is inferred).[123] While acknowledging that such expansive obligations might have potentially interfered with gatekeepers' IP and trade secrets, they could have been constructed using a more audit-based model drawing on measures such as read-only and time-limited APIs for oversight bodies, encrypted or tiered access, and purpose-limited access enquiries.

Similarly, existing portability and, where applicable, interoperability obligations[124] could have also included access to and portability of social graphs and identity credentials, recognising them as strategic infrastructural assets in the data value chain and as key components in the manifestation of potential harm.[125] Finally, to account for relational harm in enforcement actions, one could propose the development of a collective harm impact assessment tool, modelled on the DPIA framework and introduced through a regulatory sandbox mechanism or as a part of compliance report obligations.[126] These proposed measures could help to shift the focus away from a static snapshot of the emerged power constellations towards a more nuanced and dynamic understanding of sources and drivers of such power in terms of the network architecture.

In the same vein, cryptographic and programmable means of the architecture could serve as tools to reinforce the commitment to respect for individual dignity and the autonomy of users. For example, one could propose encoding consent in a granular and verifiable manner using smart contracts, allowing data subjects to express, track, and withdraw it in a technically enforceable way. More specifically, smart-contract-based consent could be integrated across the network, drawing on its structural components such as the identity layer as well as API data access points. Within the former, verifiable credentials could be used to authenticate and

[122] Arts. 6(8), 6(9), 6(10).

[123] To some extent, Art. 6(8) already reflects this logic by requiring that performance measurement data shall be provided "in a manner that enables advertisers and publishers to run their own verification and measurement tools to assess the performance of the core platform services provided for by the gatekeepers". However, the scope of Art 6(9) is rather ad-tech specific, arguable underspecified, and is not generalisable across 6(9) and 6(10)) requirements.

[124] e.g. DMA Arts 6(9), Art. 7 read in light of Art.53(2) review mandate.

[125] with due regard given to technical and organizational measures meant to accommodate data protection considerations. One of the design solutions could be the use of proxy token instead of direct identifiers to notify the members of one's social graph and collect respective consents

[126] Under, for example, DMA, Art 11

register individual privacy choices,[127] while the latter could be employed to enforce consent limitations before releasing any data to external parties.[128]

While these proposals remain necessarily exploratory, they are intended less as defined solutions and more as conceptual challenges and offerings, serving as an invitation to rethink the available regulatory means of governing Big Tech. By extending the regulatory space to include embedded logics and affordances of the digital ecosystem itself, this chapter seeks to move beyond surface-level or top-down compliance demands. In doing so, it hopes to contribute to the ongoing discourse by offering a more inclusive and grounded perspective on the underlying causes for and the actual reach of the regulatory intervention.

[127] In line with discussion in, e.g. Nguyen Binh Truong and others, 'GDPR-Compliant Personal Data Management: A Blockchain-Based Solution' (2020) 15 *IEEE Transactions on Information Forensics and Security* 1746

[128] On explanation of APIs for data access see Olga Kokoulina, 'Towards Future-Proof, Rights-Respecting Automated Data Collection: An Examination of European Jurisprudence' (2024) 26 *Vanderbilt Journal of Entertainment and Technology Law* 1