

Spilker, Hendrik Storstein; Reppen, Maria

Article

Clash between law power and code power: The case of Norway vs. Meta

Internet Policy Review

Provided in Cooperation with:

Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Spilker, Hendrik Storstein; Reppen, Maria (2026) : Clash between law power and code power: The case of Norway vs. Meta, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 15, Iss. 1, pp. 1-23, <https://doi.org/10.14763/2026.1.2078>

This Version is available at:

<https://hdl.handle.net/10419/337510>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by/3.0/de/deed.en>



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

Clash between law power and code power: The case of Norway vs. Meta

Hendrik Storstein Spilker *Norwegian University of Science and Technology (NTNU)*
Maria Reppen *Norwegian University of Science and Technology (NTNU)*

DOI: <https://doi.org/10.14763/2026.1.2078>

Published: 5 February 2026

Received: 18 December 2024 **Accepted:** 20 May 2025

Funding: The authors did not receive any funding for this research.

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Spilker, H.S., & Reppen, M. (2026). Clash between law power and code power: The case of Norway vs. Meta. *Internet Policy Review*, 15(1). <https://doi.org/10.14763/2026.1.2078>

Keywords: Platform power, Internet regulation, Surveillance advertising, Privacy, Marketing

Abstract: In this article, we analyse the controversies leading up to and following Meta's introduction of the infamous "pay or okay model" for Facebook and Instagram users in the European Union/European Economic Area (EU/EEA) region. In particular, we focus on the central role of the Norwegian data protection and consumer authorities and the unfolding of the events in the time period from the summer of 2023 to the spring of 2024. With a theoretical departure point in critical platform studies, we perform a framing analysis of the arguments employed by the central actors in the controversy in this period, which, in addition to the Norwegian authorities and Meta, include the European consumer umbrella BEUC. Furthermore, in the discussion section of the article, we address the dynamics between the various forms of power at actors' disposal to understand the anatomy of the clash between code and market power on one hand and regulatory power on the other, or, in other words, between US Big Tech and European law and policy. Thus, the article is a contribution to knowledge about how powerful platform companies employ their code and market power in phases of discussing regulation of their businesses.

Introduction

On 4 July 2023, the EU Court ruled that behaviour-based advertising carried out by Meta takes place in a way not compliant with EU law (*Meta v. Bundeskartellamt*, C-252/21). Based on this, the Norwegian Data Protection Authority (NOR-DPA) took an urgent decision against Meta on 14 July for illegal collection of user information, ordering the company to pay daily fines of NOK 1 million (~€90,000/day) until they changed their practices. Meta appealed the decision, and the parties met in Oslo District Court in August, where the decision was upheld. Later, in the autumn of 2023, the European Data Protection Board (EDPB) decided that the Norwegian decision should be made permanent and applied to the entire EU/EEA area.¹In response, Meta launched its infamous "pay or okay" solution, which, it argued, met the requirements of the decision (D'Amico et al., 2024). However, throughout the winter of 2024, Norwegian and European consumer organisations directed several complaints against Meta's new model, criticising it for not being in accordance with and circumventing the basic principles on which the decision was based.

Privacy activists have long worried about the more or less unrestricted collection of personal data by big tech companies, and have gradually been followed by public authorities (Crain, 2021), with the EU as a global spearhead, that, through clarification and tightening of the legislation, have tried to set clearer frameworks for the platforms' operations (Bradford, 2023). However, it seems almost in the nature of big platforms to look for ways to resist and sidestep attempts to regulate their businesses (see e.g. Crain, 2021; Gorwa et al., 2024, Weigl & Guzik, 2025). Earlier we conducted a case study on YouTube/Google's attempts to counter the copyright formulations in EU's new Digital Single Market Directive (DSM), through overt and (mostly) covert means, using their position and resources as a platform owner to mobilize their own users and feed a massive protest campaign against the directive (Riise et al., 2025). The case of Norway-vs.-Meta has some interesting parallels, in the manner that Meta, as a platform (and infrastructure) owner, has tried to use its position and resources to outmanoeuvre legislative intentions. The conflicts between Meta and European regulatory authorities over surveillance advertising have grown into one of the major struggles in the digital world. Our analysis offers a close-up view on an important part of that history.

Within the growing field of platform studies, a lot of important work on digital platforms, their strategies, workings and consequences has been conducted. A sub-

1. Norway, together with Iceland and Liechtenstein, are not members of the EU. They are part of the European Economic Area (EEA), which links them into the EU internal market governed by the same basic rules.

stantial body of research has revealed how platforms are working to expand and extend their power and exercise control over the larger ecosystems in which they operate, e.g. by the eradication of competitors, vertical expansion, the setting of industry standards, and political lobbying (see e.g. Vaidhyanathan, 2011; Van Dijck et al., 2018; Zuboff, 2019; Helmond et al., 2019; Nieborg et al., 2024). Comparatively, there has been less research into how platforms consolidate and defend their power (see e.g. Crain, 2021; Flew & Martin, 2022). In this respect, studying the attempts of public authorities to regulate and set boundaries for the activity of platforms is of paramount interest.

Our key research question is: *What arguments did the actors involved in this controversy employ, and with what forms of power were the actors able to enforce their arguments?*

In order to answer this, we will perform a frame analysis of arguments employed by the actors involved in the controversy as the dispute moved back and forth between Meta and various regulatory bodies. In the discussion part, the frame analysis will be connected to the various forms of power the actors posited and set in motion, and then conclude with an assessment of the outcome and its implications. Empirically, our study is based on a document analysis of key statements (case documents, legislative decisions, press releases, information letters, blog posts) associated with the case (see method section for details).

Behavioural advertising and the EU regulatory context

Our study is inspired by and constitutes an answer to Nieborg and colleagues' (2024) call for more concrete studies of the localisation of platform power in an earlier issue of this journal. In order to locate power, we need to differentiate between various forms of power. Lessig (1999, 2004) makes a distinction between four competing types of power in the digital world. Or, in other words, Lessig distinguishes between four different forms of regulation of digital spaces. In this article, however, we will refer to them as different forms of power, focusing not on their formal properties, but on their performative effects. Within the confines of the platforms – and the connected ecosystems – the owners can, and do, set the premises for access and rules of conduct at their own discretion. Adopting Lessig's typology, the platforms are performing *code power*. However, there are certain limits to this power. Platform owners must operate within the (stretchy) limits of what their users can tolerate (*norm power*) and consider the actions of competitors (*market power*). Finally, they must comply with the legislation of the countries in which they operate (*law power*).

On all popular platforms, users are granted some autonomy to search for and select information of their own choosing. To a large degree, the platforms' initial appeal rests on these possibilities. However, platforms have developed increasingly advanced, and covert, algorithms to automate the selection of content, thereby steering and nudging users in certain directions, leading Pasquale (2016) to suggest that we are living in a "black box society". For most social media platforms that have advertising revenue as their main source of income, their power and value creation is largely linked to their ability to connect users and advertisers. In order to accomplish this, platforms gather a large amount of information about their users, their characteristics, preferences, and activities.

Carah et al. (2024) describes the intensified exploitation of all possible types of behavioural data throughout the 2010s up till today as a transition *from targeted to tuned advertising*. Targeted advertising was primarily utilising static personal information, and information that the users had provided knowingly, such as gender, age, residence, interests, and more. Tuned advertising, on the other hand, uses of the continuous traces users leave, often unknowingly and without consent, through their online activities, and indirectly about their physical movements and offline lives, in order to provide a dynamic, persistent flow of advertisements that "responds to their emotions, vulnerabilities, past purchasing habits, and the time of the day" (Brown et al., 2024: p. 14).

The extensive and intrusive data collection techniques that the platform companies employ to extract personal information from users' digital traces for advertising purposes have led scholars to label these practices "*surveillance advertising*" (Bodle, 2016; Crain, 2021). Zard defines surveillance advertising as involving "monitoring the behaviour of a consumer (or an internet user), algorithmically inferring their interests and traits (often referred to as 'profiling'), and matching them with advertisements" (2024, p. 2). In her much-cited book *The age of surveillance capitalism*, Zuboff (2019) singles out these practices as evidence of the emergence of a new form of capitalism that invades people's privacy to an unprecedented degree.

Zuboff was not the first to express concern about how digital platforms were violating privacy rights of citizens. Already in the late 1990s, civil society groups fought against the way platforms collected user data for advertising purposes, and it was discussed in several parliamentary hearings both in US and EU in the 2000s, but by and large platform companies were successful in maintaining self-regulation (Crain, 2021). However, revelations in the 2010s of the platforms' transfer and trading of personal data caused acute concern among EU politicians about US companies violating the privacy rights of EU citizens. Thus, the EU institutions de-

voted themselves with greater gravity and intensity to the task of revising the legislation regulating the digital field and the activities of the platform companies.

The adoption of the General Data Protection Regulation (GDPR) in 2016 significantly strengthened personal data protection within EU/EEA and governed the transfer of personal data outside EU/EEA (Laurer & Seidel, 2021). GDPR was a response to the rapid technological advancements in digital tracking and data exploitation. It sought to give EU individuals greater control over their personal data, establishing rights to access, rectification and erasure of information gathered by platform companies, and introduced consent requirements for the collection of personal data.

The GDPR framework also represented an attempt to harmonise data protection laws across the EU and put an end to inconsistent enforcement across member states. It entailed a set of supervisory mechanisms to ensure this. Each member state of EU/EEA (including Norway) must establish at least one independent public authority responsible for monitoring GDPR compliance within its jurisdiction. When a company operates in multiple EU countries, GDPR uses a “one-stop-shop” mechanism, appointing one lead supervisory authority, usually in the country of the company’s main establishment in the EU. Meta’s European headquarter in Europe is in Ireland, thus the Irish DPA has been the lead supervisory authority in cases involving Meta. Furthermore, if there are disputes between different DPAs, the European Data Protection Board (EDPB), made up of heads of all national DPAs, are called in to issue binding decisions.

GDPR was widely hailed as a piece of legislation that could protect European citizens’ privacy against aggressive online actors. However, as with most new legislation, its scope and practical application had to be interpreted and clarified. The next step was thus to test the legislation against what was claimed to be under-regulated and highly worrisome personal data collection practices by the social media platforms in general, and Meta, as the biggest player, in particular. On 25 May 2018, the GDPR had been made legally effective in all member states of the EU/EEA. On the same day, the digital rights organisation Noyb (“Not In My Backyard”) filed a complaint to the Austrian DPA against Meta’s attempts ahead of the implementation of the GDPR to circumvent the consent requirements in the legislation.

In accordance with the supervisory rules, the case was transferred to the Irish DPA, which started litigation. In 2021, after three years of investigation, it published a draft decision in favour of Meta’s arguments for maintaining and continuing its da-

ta collection practices. The Irish DPA had already been heavily criticised by other European DPA's for being slow, and the draft was perceived as overly deferential to Meta. Thus, the Irish DPA referred the case to EDPB, who in a binding decision went against the Irish interpretation.

Following the EDPB's binding decision, on 31 December 2022, the Irish DPA issued a €390 million fine to Meta and gave the company three months to bring their practices in compliance to the GDPR. In response, Meta once again updated its terms and conditions while continuing to process personal data as before (see Zard for a detailed analysis, 2024). However, in a parallel process, the Bundeskartellamt, the German competition authority, prohibited Meta from combining personal data from different sources without consent. Meta appealed the decision to the EU Court, who on 4 July 2023 ruled that the behaviour-based advertising carried out by Meta is illegal under GDPR. This is the point where NOR-DPA enters into the story.

Method: Follow the case!

Our interest in the case was initially triggered by the surprise we experienced when we learned from a news story that NOR-DPA were filing a lawsuit against Meta. How did the little country Norway dare to challenge the giant company Meta, and what did the authorities think they could achieve? From this initial curiosity, we “followed the case” (Latour, 1987) and traced it both back and forth in time, gathering whatever information we could find, whether press releases, policy papers, news coverage, court documents, information letters, organizational blog posts, Meta's terms of use, the central articles of the GDPR regulation, or other materials.

Interestingly, the traces we followed took us out of Norway on several occasions, to Ireland, Belgium, and other EU countries. Also, we learned that the case had antecedents far back in time – and it was still ongoing during the data collection period. Our analysis focuses mainly on the period from the start of the legal process in Norway in July 2023 to the end of February 2024. After the data collection, we had gathered a large and diverse pile of documents. We limited the analysis to documents published or made available on the websites of the central actors, whilst media articles and court documents were omitted. A total number of 29 documents were analysed. A full and numbered overview of the analysed documents is found in the appendix. In the analysis, the documents are identified by these numbers.

The four “main” actors in our analysis were the Norwegian Data Protection Authority (NOR-DPA), Meta, the Norwegian Consumer Council (NOR-CC), and the Bureau Européen des Unions de Consommateurs (BEUC).

In the first step of the analysis, we examined the material we had collected to reconstruct the unfolding of the controversy over time, including its prelude. In the second step, we performed a frame analysis of the arguments of various parties, and investigated how the arguments had developed over time (Björnehed & Eriksson, 2018). We conducted a close reading of the central documents explicating the views of each of the key parties. In the initial frame analysis, we looked for how the parties were defining Meta’s collection of personal data, the purpose, the problem, moral, and legal basis, responsibilities and policy solutions (Kitzinger, 2007).

During the coding process, we discovered that the parties almost always anchored their viewpoints in generative frames, in general and well-known, legal and societal frames (Ihlen & Allern, 2008). The five central frames in our material were:

1. The privacy rights frame
2. The consumer rights frame
3. The democracy frame
4. The service quality and consumer satisfaction frame
5. The necessary for business frame

We found that the parties were negotiating both about which frames should be given the most weight *and* about which interpretations of the various frames were valid interpretations.

In the final step of the analysis, we connected the use of frames to the means of power at the actor’s disposal.

Analysis

The struggle between Meta and European regulatory authorities over surveillance advertising is one of the major struggles in the digital world. Zard (2024) calls the article where he analyses the unfolding of controversy from 2018 up to the EU Court decision on 4 July 2023 for “Five years of illegitimacy of surveillance advertising”. However, as it would turn out, the struggle did not end there.

Like other DPAs, NOR-DPA had increasingly grown impatient with the Irish DPA through the long process from 2018. And when the Irish DPA did not follow up the court decision of 4 July immediately with sanctions against Meta, NOR-DPA decid-

ed to take unilateral action. The following analysis offers a close-up view on the events that followed.

The Norwegian Data Protection Authorities – July to September 2023

On 14 July 2023, NOR-DPA filed their urgent decision to ban Meta’s behavioural advertising practices on 14 July 2023 (8, 9). The decision to use the “urgent decision” clause in the GDPR, instead of leaving further legal proceedings to the IRE-DPA, was an unusual step, and the use of this clause required weighty arguments. The letter informing Meta about the ban also contained several sharp accusations against Meta: “The persistent state of non-compliance [...] demand[s] immediate action to protect the rights and freedoms of Norwegian data subjects. [If a continued] delay in remedying that violation [should] be permitted, data subjects would be at acute risk and in practice lack effective protection under the GDPR” (8: p. 3). The decision had a temporary duration of three months, with daily fines of NOK 1 million (approx. 90,000 Euro) in case of non-compliance.

Some predicted that Meta would now suspend Facebook and Instagram for Norwegian users. However, NOR-DPA cooperated closely with data protection authorities in other EU/EEA countries. When it became clear that Meta was ignoring their decisions, NOR-DPA asked the joint European Data Protection Board (EDPB) to extend the decision to the entire EU/EEA area (11).

NOR-DPA were using primarily *the privacy rights frame* and *the democracy frame* in their arguments against Meta. In the introduction to the letter of order to Meta (8), they started by explaining how they, as a data supervisory authority, were responsible for ensuring that fundamental human rights are safeguarded in the digital field. When they later went into greater detail about the legal background for the case, they showed how these fundamental rights are enshrined in both Norwegian and European law, and then pointed out how the GDPR was related to these: “GDPR gives effect to these fundamental rights” (ibid.: p. 6). Meta was accused of breaking a range of the principles laid down in the GDPR to ensure the *safeguarding of privacy rights*: principles of fairness and transparency, purpose limitation, data minimization, confidentiality, integrity and storage limitation. NOR-DPA provided a principled and normative interpretation of privacy to justify its involvement in the case. The ruling on Meta was hard: “The intrusive commercial surveillance for marketing purposes is one of the biggest privacy risks on the Internet today” (9).

Furthermore, the inspectorate noted that the surveillance took place without in-

formed consent. Admittedly, there were some opportunities to opt out of parts of the data collection, but “[d]ata protection tools are generally hidden away from sight so that in practice they are effectively reserved for a minority of motivated data subjects looking for them” (8: p. 22). Ordinary users lacked the tools to assert sufficient control over their own data. In relation to vulnerable groups, this was even more critical: “Since the tracking takes place covertly, it is difficult for most people to understand [it]. In addition, there are many unusually vulnerable people who use Facebook and Instagram who need special protection, for example the young, the elderly and those with cognitive impairments” (9).

In their argumentation, NOR-DPA also placed a lot of emphasis on the importance of Meta's data processing and advertising practices *in a democratic perspective*. They accused Meta of being unwilling to discuss the potential consequences of the filtering and personalization of content, which is based not only on users' gender, age, location, and so on, but on all the hidden surplus information they surreptitiously provide in their interaction with the platform: “[It] may *prevent* certain data subjects from seeing information that is available to other data subjects. There is no assessment of how this may reinforce stereotypes or how it may affect political participation” (8: p. 19).

In a later press release, the inspectorate elaborated on this point: “When Meta decides which ads you get to see, they also decide which content you don't get to see. This affects freedom of expression and information in society” (9). The large role Meta's platforms have taken on in many Norwegians' lives, in almost all areas, makes this all the more worrying: “Many interact with content related to, for example, health, politics and education, and there is a danger that this too is used indirectly to adapt marketing to them” (ibid.). NOR-DPA also points out: “Behaviour-based targeting of political advertisements in connection with elections is particularly problematic from a democratic perspective” (ibid.).

Meta – August to November 2023

After NOR-DPA's ban, events unfolded in rapid succession. Meta sued NOR-DPA in Oslo District Court on 3 August for what they claimed was an erroneously imposed order (Meta Platforms, Inc. v. Norwegian Data Protection Authority)(21). The Oslo District Court made a judgment in the case on 6 September, ruling in favour of NOR-DPA (9). Then, on 27 October EDPB finalised their ruling on the request from NOR-DPA, finding that Meta's current practices represented a grave violation of the GDPR that justified “a derogation from the usual cooperation procedure which can only be used in exceptional circumstances” (16). Thus, the board decided that the

temporary Norwegian decision should be made permanent and extended to the whole EU/EEA area with immediate and binding effect (17). Now Meta had to react.

Meta had been prepared for such a decision and launched their response a few weeks later: the rollout of the “*pay or okay model*”. On 30 October and the consecutive days, all EU/EEA users of Meta’s platforms were met with a pop-up window offering – or, more exactly, demanding – that they choose between two alternatives: Either they could continue to use the platforms as before, for free, but with ads – or they could sign up for an ad-free subscription. The subscription would cost €12.99/month (with an addition of €8/month that would come into effect later per additional profile for users with multiple profiles) (22, 23). In a press release, Meta defended their existing practices: “We believe in an ad-supported internet, which gives people access to personalized products and services regardless of their economic status” (22).

Reasonably, Meta also related to *the privacy frame* since it is the main point of appeal against them in this controversy. In their responses to the accusations against them, they followed two lines of argument: First, that they have always taken users’ privacy into account. When they appealed the decisions of the inspectorate before the Oslo District Court, they insisted that the users’ privacy had already been safeguarded. They boasted that they had made improvements so that users can “opt out of having certain kinds of data used to inform the ads they see” and “bulk delete content they’ve posted [...] to manage their digital footprints” (23). However, they did not mention anything about what the users can do with the invisible data, the behavioural surplus data, which the company collects, or that this is collected by default without explicit and informed consent.

In addition, part of their privacy argumentation consists of claims that the requirements from NOR-DPA and other European regulators are unclear and inconsistent, go beyond what is required in the GDPR and DMA, and thus are difficult to deal with: “Given that regulators themselves disagreed with each other [...], it is hard to understand how we can be criticized for the approach we have taken to date” (23). Later, in connection with the announcement of the “pay or okay” model, they were more conciliatory in their wording: They “respect the spirit and purpose of these evolving European regulations and are committed to complying with them” (22). But there was a “but” in the goodwill.

Meta used several other arguments to defend its basic business model and data collection practices. We saw that NOR-DPA used *a democracy frame* to argue that

Meta's practices constituted a threat. Meta promoted a completely different view of its role for democracy. They bragged proudly: "At Meta, we believe that technology is about giving everyone a voice" (22). However, the only way to do that was to continue to deliver an ad-based service: "We are committed to an ads-supported digital business model, because it is the cornerstone of an inclusive internet where everyone can access online services and content for free" and "regardless of their economic status" (ibid.). Freedom is linked so closely to personal marketing that the two are almost equated: "[An ad-based service] allows people to use services like Facebook and Instagram for free whilst benefiting from seeing personalized advertising, helping them discover new products and brands that are most relevant to them" (ibid.).

Meta probably also bet that most users were just as interested in a useful and customised service as in a democratic and open service. *The service quality and consumer satisfaction frame* was a third important element in the executives' argumentation. For individuals, they emphasised the "tailored" experience which they offered. The intrusive information gathering was presented only as a means to make Meta's services as well adapted to each individual as possible: "Facebook and Instagram are inherently personalized, and we believe that providing user with their own unique experience – including the ads they see – is a necessary and essential part of that service" (23). They delivered the following answer to regulators who expected them to make the same information democratically available to all users: "It would be highly unusual for a social media service not to be tailored to the individual user" (ibid.).

The press releases from Meta in this case make interesting reading, looking at the way the company tries to instruct users, reassure advertisers and convince regulators at the same time. In the following quote, Meta tries both to convince users to continue with the ad-based version and to keep advertisers on board: "And we remain steadfast in our view that personalized ads are the best experience for people and businesses – and because people understand that value, we expect that most people will choose our personalized ads service even with these expanded options" (22). To bolster their argument, the company claimed to have the research on their side – albeit without concrete references: "Studies show that people and businesses prefer personalized ads which support jobs and economic growth, and give people access to free online services" (ibid.) (in fact, study is conducted by Meta employees and ex-employees).

These latest quotes bring us into the fourth frame Meta used in their argument: *the necessary for business frame*. Basically, this is a standard argument with which

companies almost automatically counter demands for regulation of their businesses. It is, however, quite striking how Meta have avoided highlighting the necessity of the data collection they conduct for their own business but instead points to its necessity for other businesses.

On the other hand, Meta's services are of great worth to the European business community: "It also allows small businesses to reach potential customers, grow their business[es] and create new markets, driving growth in the European economy" (ibid.). Meta could quantify this value: "In Europe, every Euro spent on our ads drives on average 3.37 Euros in revenues for advertisers, supporting over €84 billion in business revenues every year" (ibid.). However: "This value is only available through personalized advertising but is at risk of decline because, if EU regulation makes digital advertising less efficient, the entire European business community suffers" (ibid.).

NOR-CC and BEUC – November 2023 to February 2024

The "pay or okay model" was not well received by the Norwegian Consumer Council (NOR-CC) or other consumer councils. On 30 November, they submitted, together with 18 other European consumer councils, a complaint about Meta's solution to the Consumer Protection Cooperation Network (CPC), the joint network for EU/EEA consumer authorities (1, 18). The main reason why NOR-CC "took over" NOR-DPA's role as a watchdog, seems to have been that with "pay or okay", Facebook and Instagram were now also offered as subscription-based paid services and thus fell under consumer legislation. At the same time, a central part of the argumentation of the consumer organizations was that these platforms had been paid services all along, only that the means of payment in the "free" versions was the users' personal information. NOR-CC worked in close cooperation with other European consumer councils and BEUC, their umbrella organization, and are treated as one in this section.

In the complaint, NOR-CC argued: "Meta's practice portrays privacy as a right for which we must pay. We expect the authorities to state clearly that fundamental rights are neither for sale nor something that companies can choose whether they want to deal with [it or not]." Furthermore: "[The pay or okay model] gives consumers a false sense of control over their own privacy. The company also pressures users to choose before they gain access to their accounts" (18).

A few months later, on 29 February 2024, the NOR-CC, together with seven other consumer councils and coordinated via BEUC, the joint umbrella agency for inde-

pendent European consumer organizations, submitted a new complaint against the “pay or okay model” – this time to the respective national data protection authorities. Whilst the first complaint held that Meta, through “unfair, deceptive and aggressive marketing practices [...] imposed a fake choice on consumers” (19), this time the complaint attacked the perpetuation of illegal data collection practices breaching the GDPR. The “pay or okay” model was portrayed as a “smokescreen to obscure the real problem of illegal processing of data” (19, see also 3).

NOR-CC and BEUC’s argumentation was conducted within *a consumer rights frame*, concerning the specific rights that individuals have as purchasers and users of commercial goods, and which are laid down in separate consumer regulations. Firstly, Meta was criticized for misleading practices. While “pay or okay” was marketed as a choice between a free and a paid option, this was misleading because “it has been determined in several court cases that users pay with their personal data anyway” (18). Furthermore, the offer of a payment option was presented as if it solved the problem of illegal tracking and profiling. In reality, the consumer organizations argued, only the advertisements disappeared, not the underlying collection of personal data. This could still be used for other purposes, for example behaviour-based advertising to the user’s contacts or people with the same demographics.

Secondly, Meta was criticized for aggressive marketing. This criticism was rooted in the way the subscription solution was presented to users when they accessed Meta’s respective platforms, through a pop-up window without the possibility to ask for more time to think about it, or to use the service in the meantime. Meta was “creating a sense of urgency, Meta pushes consumers into making a choice they might not want to take” (1). Given the price of the payment solution, it is likely that Meta calculated that this would make most users stay with the ad-based solution.

Thirdly, the misleading and aggressive marketing deprived users of the opportunity to make an informed choice, as consumer legislation requires them to be able to. Both data protection and consumer organizations had long demanded that Meta offer users the opportunity to consent to the collection of personal data, which had been absent until then. Meta claimed that they had answered this objection with their new solution. The consumer organizations did not agree: A consent had to be “freely given, specific, informed and unambiguous” (3) and Meta failed on all these requirements. On the contrary, consent had to be given under circumstances bordering on coercion: It had to be done quickly, without sufficient information, and without the possibility of consideration or any easy means of re-

versal.

In the February complaint, the consumer organizations elaborated on the criticism of Meta's underlying data collection practices and the absence of the information about what they consist of. The “pay or okay model” was portrayed as a “smoke-screen to obscure the real problem of illegal processing of data” (19). “Meta keeps consumers in the dark about its data processing, making it impossible for the consumer to know how the processing changes if they choose one option or the other.” (3). Pay or okay has not really changed anything and NOR-CC were running out of patience: “[Meta’s] business model, which is based on massive monitoring and profiling of users, is fundamentally at odds with European and Norwegian law. Unfortunately, the company clearly has no intention of changing its business model or adapting to current regulations” (19).

An important change took place in the aftermath of our initial data collection: As a result of the continued complaints and demands from European regulatory authorities, Meta was forced to adjust its original model. On 12 November 2024, Meta announced the following changes to the pay or okay solution: from now on, users would be able to choose between three options: the subscription solution (where prices would be reduced by 40%), as well as two different ad-based solutions (22). The first ad-based solution would be as before. In addition, users would be given the opportunity to choose a “less personalized ads” version, using only contextual information (“what a person sees in a particular session”) and a few personal data points that users had provided knowingly, such as age, gender, and location. This version comes with a warning: It will, unlike the personalized ad-version, include non-skippable ads. In a press release of January 2025, BEUC argued that the new version of Meta’s pay-or-consent policy failed to address the fundamental problems identified in the tech giant’s pay-or-consent initial approach (30). However, it appears that Meta still refuses to make changes to – or disclose – its basic data collection procedures.

Discussion

In the controversy between Meta and Norway/EU, the data protection inspectors and the consumer councils have appeared strongly critical and unilaterally negative towards Meta's operations. Meta has been more diplomatic in its responses – even though it has been accused of both sidestepping, delaying, and evading all demands. Meta’s strategy has probably been to try to rhetorically dampen the confrontation in order to keep their foothold in Europe with the least possible changes to their business operations. However, one can sense that the constant

criticism is starting to wear on patience when Meta in an October 2023 press statement writes: “Despite our concerted efforts to comply with EU regulation, we have continued to receive additional demands from regulators that go beyond what is written in the law” (22).

A range of different frames has been employed by the parties on both sides of the controversy. NOR-DPA criticize Meta based on a *privacy rights frame* in which Meta's advertising-based business model and the underlying collection and processing of user data are said to violate universal rights, as well as a *democracy frame* in which major questions are raised about bias in the kind of information Meta's personalization algorithms give users access to. NOR-CC and its sister organizations' objections are based on a *consumer rights frame* in which Meta is accused of illegal and misleading marketing as well as the collection of personal data without the users' consent.

Meta, on the other hand, appeals to a series of different frames in defence of its business. It also relates, necessarily, to the *privacy rights frame*, but tries to promote a far more limited interpretation where users' possibility to delete their own posts are highlighted as a prime example of privacy protection. At the same time, Meta tries to steer attention away from and obfuscate their own data collection practices. The company also appeals to a *democracy frame* but again emphasises completely different elements to NOR-DPA. Meta argues that the very basis of its enterprise, the ad-based and personalized business model, is fundamentally inclusive and democratic per se, because it enables universally free access and participation. In addition, the company applies a *service quality and consumer satisfaction frame*, where it argues that users want the existing free service because it provides them with the most useful and best-customized experience, and a *necessary for business frame*, where Meta portrays itself as a benefactor of European business.

The choice of frames – and the distinct interpretations – are linked to the unequally distributed instruments of power at the actors disposal. Lessig's (2004) distinction between *four forms of platform power – law, code, market and norm* – are fruitful distinctions for discussing these differences and their significance for the course of the controversy.

The main form of power that the data protection authorities and consumer councils have at their disposal is *law power*. They have in tandem attacked Meta with a basis in different variants of law power, anchored in Norwegian and common EU/EEA legislation. The personal data protection regulation GDPR, and recently also the digital markets and services regulation DMA, have been central in challenging

Meta's business model, information collection and data processing. Based on the data protection and consumer organizations statutory powers, they have been able to force Meta to meet them on an away match.

It is important to remember that this "Norway-vs-Meta case" is part of a larger process, a persistent and ongoing struggle in which European regulatory authorities have tried to gain better control over and set clear frameworks for the multinational, and usually US-based, platforms' operations in Europe (Bradford, 2023; Crain, 2021). The case against Meta has, as we mentioned at the outset, a longer history that stretches back to the introduction of the GDPR in 2018 and the testing of the legislation against Meta's data collection practices in the years that followed (Zard, 2024). The "Norway vs. Meta" case has taken place in the extension of this and can therefore be considered the final round in the first major test of the robustness of the GDPR in meeting with international Big Tech.

In light of this, the response Meta finally gave, after years of evasion and deferring, is particularly illuminating. What Meta did with the introduction of the pay or okay model is, in Lessig's terms, to use *code power* against law power. This is exactly what Lessig had warned about twenty years earlier when he was criticizing the methods used by the rising technology industry to override national laws and regulations and dictate the rules of the digital world.

During our research, we have been surprised on two occasions: The first was when Norwegian supervisory authorities took legal action against Meta; the second was when Meta responded with the pay or okay model. Clearly, this was not the answer the Norwegian Data Protection Authorities expected either. NOR-DPA demanded a general change to the data collection practices. Meta instead used their control over the platform code to impose upon users a forced choice between ads and subscription instead. We can say that Meta moved the entire match to their home ground. However, unlike some of the cases Lessig wrote about at the turn of the century, the official authorities did not stand back idly and bewildered. Through the legal complaints from the consumer councils, and later the European Data Protection Board (EDPB), Meta has been forced to make further changes to its business practices in Europe. The clash between law and code is still ongoing.

Lessig's third form of power is *market power*, the power actors possess through their position in the market. We can note that Meta's market power has not been to their advantage in our case. Of course, in their formal responses to the NOR-DPA, they predictably point to the benefits of their services for consumers and European businesses. However, it was precisely because of the dominant position of

their platforms with European users and in the European advertising market that they became a prime target of EU/EEA's regulatory efforts and a testing ground for the reach of GDPR. There has been a lot at stake for Meta. The original judgment from IRE-DPA, on behalf of the entire EU/EEA, and the Norwegian emergency decision that the EDPB extended to the entire EU and made permanent, could risk threatening Meta's position in the European advertising market, as well as potentially having a "contagion effect" to other markets, on a global scale.

It is in this light that we must understand the use of "the necessary for business frame" directed at European companies and how much they earn from marketing through Meta's platforms – an attempt to activate corporate pressure from industry and business organizations against placing too strict restrictions on Meta's operations. Based on our material, it is difficult to determine whether Meta's market position has had any positive effect for Meta on the decisions in this case. But it cannot be ruled out that it has protected them from even more drastic and intrusive restrictions.

Finally, let us note that *norm power*, somewhat surprisingly, has played only a small role in the controversy. For Lessig, norm power is the slightly imprecise term for the power users have through the overall pressure of their actions, attitudes, behaviour and norms (e.g. through protests against decisions, by simply leaving a platform, or staying loyal and conform). There are a number of examples in the digital field where user engagement and protests have had a definitive influence. An example with parallels to our case is the engagement from YouTube users in 2018-2020 against parts of the proposal for the EU's Digital Market Act, which contributed to the moderation of the original draft (Riise et al., 2025). Even more recent are the massive user protests when Meta announced in May 2024 that they would use users' posts and photos to train their AI models, forcing Meta to reverse the decision (but only until June 2025).

In the controversy we have studied – and in the period we have studied it – there is nothing to suggest that involvement from users has influenced progress and outcomes. We can also add that Norwegian users, compared to users in other European countries, have generally been characterized by a strikingly low commitment to digital issues and an absence of digital activism (Spilker, 2014). In this respect, it is an additional puzzle why it has been the Norwegian supervisory authorities who, in 2023-2024, have fronted EU/EEA's efforts to regulate Meta's operations. There has been a high level of engagement from the supervisory authorities, on behalf of the users, without a corresponding engagement from the users themselves.

Conclusion

Our study is inspired by and constitutes an answer to Nieborg et al.'s (2024) call for more concrete studies of the localization of platform power. We have retrieved Lessig's old (2004) but almost forgotten and rarely used typology of forms of power to accomplish this task. We will argue, and hope to have demonstrated, that this typology, which is based on a distinction between the fundamental qualities from which power derives, provides a fruitful pathway for analysing key confronting forces in today's platformised world.

Framing analysis has provided us with effective tools to sort out and clarify the stands and moves of the parties involved. Our analysis is a contribution to knowledge about how powerful platform companies act when they are faced with regulatory proposals that could restrict their operations. Gorwa et al. (2024) discuss five different strategies that their research has identified as platforms' repertoire when facing restrictions: 1) access lobbying (direct contact with policy decision-makers), 2) coalition building (establishing industry associations to resist regulation), 3) user mobilization (engaging platform users in public protests), 4) brand building (building a more positive reputation), and 5) funding and sponsoring (i.e. funding academic research or idealistic NGO's).

This shows some of the variety of means platform companies have at their disposal and can activate when needed and appropriate. In our previous analysis of YouTube vs. the EU, we uncovered in detail how YouTube/Google used strategies two and three in their fight against the proposal for DMA (Riise et al., 2025) This case has been different. The main impression we have is that Meta has essentially stood alone but used its code power and market power to try to circumvent regulations. In particular, the use of code power reminds us of an important means of power and strategic resource in the possession of the platform companies, which should be added to Gorwa et al.'s taxonomy.

Crain (2021) has claimed that, historically, regulators have often aimed too narrowly or been too unspecific with their regulatory approaches, which has enabled Big Tech to circumvent or reduce the effects of regulations and move on as they please. This shows how important it is that the regulatory authorities make good analyses of what countermeasures the platforms may try to carry out if the regulations are to have the desired effects. The persistent pursuit of Meta after "pay or okay" may suggest that EU/EEA legislators and regulators have learned this lesson, although it is still too early to determine any final outcome and long-term effects of the controversy. However, this controversy could be groundbreaking for regula-

tors who deal with platform companies in the future, causing a change in the concentration of power that exists in the digital world today.

References

- Björnehed, E., & Erikson, J. (2018). Making the most of the frame: Developing the analytical potential of frame analysis. *Policy Studies*, 39(2), 109–126. <https://doi.org/10.1080/01442872.2018.1434874>
- Bodle, R., Hamilton, J. F., & Korin, E. (2017). A critical theory of advertising as surveillance: Algorithms, big data, and power. In *Explorations in Critical Studies of Advertising* (pp. 148–162). Routledge. <https://doi.org/10.4324/9781315625768-18>
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology* (1st edn). Oxford University Press. <https://doi.org/10.1093/oso/9780197649268.001.0001>
- Brown, M.-G., Carah, N., Robards, B., Dobson, A., Rangiah, L., & De Lazzari, C. (2024). No targets, just vibes: Tuned advertising and the algorithmic flow of social media. *Social Media + Society*, 10(1). <https://doi.org/10.1177/20563051241234691>
- Carah, N., Hayden, L., Brown, M.-G., Angus, D., Brownbill, A., Hawker, K., Tan, X. Y., Dobson, A., & Robards, B. (2024). Observing ‘tuned’ advertising on digital platforms. *Internet Policy Review*, 13(2), 1–26. <https://doi.org/10.14763/2024.2.1779>
- Crain, M. (2021). *Profit over privacy: How surveillance advertising conquered the internet*. University of Minnesota Press.
- Cunningham, S., Craig, D., & Lv, J. (2019). China’s livestreaming industry: Platforms, politics, and precarity. *International Journal of Cultural Studies*, 22(6), 719–736. <https://doi.org/10.1177/1367877919834942>
- D’Amico, A., Pelekis, D., Teixeira Santos, C., & Duivenvoorde, B. (2024). Meta’s Pay-or-Okay Model: An analysis under EU Data Protection, Consumer and Competition Law. *Technology and Regulation*, 2024, 254–272. <https://doi.org/10.71265/tkk29041>
- Flew, T., & Martin, F. (with Martin, F. R., & Flew, T.). (2022). *Digital platform regulation: Global perspectives on internet governance* (1st edn). Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-95220-4>
- Gorwa, R., Lechowski, G., & Schneiß, D. (2024). Platform lobbying: Policy influence strategies and the EU’s Digital Services Act. *Internet Policy Review*, 13(2), 1–26. <https://doi.org/10.14763/2024.2.1782>
- Helmond, A., Nieborg, D. B., & van der Vlist, F. N. (2019). Facebook’s evolution: Development of a platform-as-infrastructure. *Internet Histories* (2017), 3(2), 123–146. <https://doi.org/10.1080/24701475.2019.1593667>
- Ihlen, Ø., & Allern, S. (2008). This is the issue: Framing contests, public relations and media coverage. In J. Strömback, M. Ørsten, & T. Aalberg (Eds), *Communicating politics: Political communication in the Nordic Countries* (pp. 233–248). NORDICOM.
- Kitzinger, J. (2007). A comparison of approaches. Framing & frame analysis. In *Media studies: Key*

issues and debates.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Open University Press.

Laurer, M., & Seidl, T. (2021). Regulating the European data-driven economy: A case study on the General Data Protection Regulation. *Policy and Internet*, 13(2), 257–277. <https://doi.org/10.1002/poi.3.246>

Lessig, L. (1999). *Code: And other laws of cyberspace*. Basic Books.

Lessig, L. (2004). *Free culture: How big media uses technology and the law to lock down culture and control creativity*. Penguin Press.

Nieborg, D., Poell, T., Caplan, R., & van Dijck, J. (2024). Introduction to the special issue on Locating and theorising platform power. *Internet Policy Review*, 13(2), 1–17. <https://doi.org/10.14763/2024.2.1781>

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Riise, M., Åm, H., & Spilker, H. S. (2025). SAVE YOUR INTERNET! The persuasion work of YouTube in the controversy over EU's digital market directive. *Policy and Internet*, 17(2), n/a. <https://doi.org/10.1002/poi.3.421>

Spilker, H. S. (2014). Punks, hackers, and unruly technology: Countercultures in the communication society. In *Media and Revolt* (1st edn, Vol. 11). Berghahn Books.

Vaidhyanathan, S. (2011). *The Googlization of everything: (And why we should worry)* (1st ed.). University of California Press. <https://doi.org/10.1525/9780520948693>

Van Dijck, J. (with Poell, T., & Waal, M. de). (2018). *The platform society: Public values in a connective world*. Oxford University Press.

Weigl, L., & Guzik, A. (2025). In Brussels we trust? Exploring corporate resistance in platform regulation. *Law, Innovation and Technology*, 17(1), 335–365. <https://doi.org/10.1080/17579961.2025.2470588>

Zard, L. (2024). *Five years of illegitimacy of surveillance advertising (48kgu_v1)*. SocArXiv. <https://doi.org/10.31235/osf.io/48kgu>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. Profile Books.

Appendix: Analysed documents

1. BEUC (2023, November 30). *Choose to Lose with Meta* (BEUC) [Press Release]. <https://www.beuc.eu/choose-to-Lose-with-Meta>
2. BEUC (2023, November 30): *Consumer groups file complaint against Meta's unfair pay-or-consent model*. <https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model>
3. BEUC (2024). *The Meta Smokescreen* | BEUC. <https://www.beuc.eu/enforcement/meta-smokescreen> (accessed 2024, April 24).

4. BEUC (2024, February 29). *Consumer groups launch complaints against Meta's massive, illegal dataprocessing behind its pay-or-consent smokescreen*. <https://www.beuc.eu/press-releases/consumer-groups-launch-complaints-against-metas-massive-illegal-data-processing>
5. BEUC (2024, February 29). *European consumer groups take action against Meta for Breaches of GDPR: Letter to commissioner Breton*. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-022_Consumer_groups_take_action_against_Meta_breaches_of_GDPR_Th.Breton.pdf
6. BEUC (2024, February 29). *How Meta is breaching consumers' fundamental rights* [Press Release]. <https://www.beuc.eu/reports/how-meta-breaching-consumers-fundamental-rights>
7. Datatilsynet [Norwegian Data Protection Authority] (2023, January 5). *Overtredelsesgebyr til Facebook og Instagram*. Datatilsynet. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/overtredelsesgebyr-til-facebook-og-instagram/>
8. Datatilsynet [Norwegian Data Protection Authority] (2023, July 14). *Letter to Meta demanding urgent and provisional measures*. https://www.datatilsynet.no/contentassets/36ad4a92100943439df9a8a3a7015c19/urgent-and-provisional-measures--meta_redacted.pdf
9. Datatilsynet [Norwegian Data Protection Authority] (2023, July 17). *Midlertidig forbud mot adferdsbasert markedsføring på Facebook og Instagram*. Datatilsynet. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/midlertidig-forbud-mot-adferdsbasert-markedsforing-pa-facebook-og-instagram/>
10. Datatilsynet [Norwegian Data Protection Authority] (2023, November 8). *Datatilsynet følger med på Metas nye løsning*. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/datatilsynet-folger-med-pa-metas-nye-losning/>
11. Datatilsynet [Norwegian Data Protection Authority] (2023, October 31). *Datatilsynets vedtak mot Meta utvides til EU/EØS og gjøres permanent*. (31.10.2023). <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/datatilsynets-vedtak-mot-meta-utvides-til-eueos-og-gjores-permanent/#:~:text=Webanalyse,Datatilsynets%20vedtak%20mot%20Meta%20utvides%20til%20EU>
12. Datatilsynet [Norwegian Data Protection Authority] (2023, Oktober 25). *Meta går til ny sak mot Datatilsynet*. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/meta-gar-til-ny-sak-mot-datatilsynet/>
13. Datatilsynet [Norwegian Data Protection Authority] (2023, September 28). *Meta-saken løftes til europeisk nivå*. Datatilsynet. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/meta-saken-loftes-til-europeisk-niva/>
14. Datatilsynet [Norwegian Data Protection Authority] (2023, September 6). *Datatilsynet vant mot Meta i Oslo tingrett*. <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/datatilsynet-vant-i-oslo-tingrett/>

15. EDPB (2022, December 31). In the matter of the General Data Protection Regulation. DPC Inquiry Reference: IN-18-5-5. https://www.edpb.europa.eu/system/files/2023-01/facebook-18-5-5_final_decision_redacted_en.pdf
16. EDPB (2023, April 13). *Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR)*. https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf
17. EDPB (2023, December 7): *EDPB publishes urgent binding decision regarding Meta | European Data Protection board*. https://www.edpb.europa.eu/news/news/2023/edpb-publishes-urgent-binding-decision-regarding-meta_en
18. Forbrukerrådet [Norwegian Consumer Council] (2023, November 31). *Forbrukerrådet klager inn Metas «ja eller betal-modell*. <https://www.forbrukerradet.no/siste-nytt/forbrukerradet-klager-inn-metas-ja-eller-betal-modell/>
19. Forbrukerrådet [Norwegian Consumer Council] (2024, February 29). The Norwegian Consumer Council files legal complaint against Meta for numerous violations of the GDPR. <https://www.forbrukerradet.no/side/the-norwegian-consumer-council-files-legal-complaint-against-meta-for-numerous-violations-of-the-gdpr/>
20. Meta (2023). Privacy Center. <https://www.facebook.com/privacy/center/> (accessed 2024, April 24).
21. Meta (2023, August 1). *How Meta Uses Legal Bases for Processing Ads in the EU*. <https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/>
22. Meta (2023, October 10). *Facebook and Instagram to Offer Subscription for No Ads in Europe*. <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>
23. Meta (2024, January 22). *Offering People More Choice on How They Can Use Our Services in the EU*. <https://about.fb.com/news/2024/01/offering-people-more-choice-on-how-they-can-use-our-services-in-the-eu/>
24. NOYB (2023, November 20). *Noyb files BDPR complaint against Meta over “Pay or Okay”*. <https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay>
25. NOYB (2023, October 3). *Meta (Facebook/instagram) to move to a “Pay for your Rights” approach*. <https://noyb.eu/en/meta-facebook-instagram-move-pay-your-rights-approach>
26. NOYB (2024, January 11). *Meta ignores the users’ rights to easily withdraw consent*. <https://noyb.eu/en/meta-ignores-users-right-easily-withdraw-consent>
27. NOYD (2023, July 4): *CJEU declares Meta/Facebook’s GDPR approach largely illegal*. <https://noyb.eu/en/cjeu-declares-metafacebooks-gdpr-approach-largely-illegal>
28. NOYD (2024, Mars 19). *“Pay or okay”: 1,500 € a year for your online privacy?* <https://noyb.eu/en/pay-or-okay-1500-eu-year-your-online-privacy>

29. Oslo Tingrett [Oslo District Court] (06.09.2023). Kjennelse i saken Meta versus Datatilsynet. Kjennelse angående begjæring om midlertidig forføyning mot Datatilsynets Vedtak, Personvernsforordningen, sak nr. 23-114365TVI-TOSL/08 og 23-114359TVI-TOSL/08 [Verdict]. <https://www.datatilsynet.no/contentassets/4096b3bd53094eb5bf2c184bd6ae4aef/avgjorelse-i-oslo-tingrett-060923.pdf>
30. BEUC (2025, January 23). Consumer groups red card Meta's latest pay-or-consent policy. <https://www.beuc.eu/press-releases/consumer-groups-red-card-metas-latest-pay-or-consent-policy>

Published by



in cooperation with



Universitat Oberta de Catalunya

UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies