

Concurrences

COMPETITION LAW REVIEW

Payments for personal data in the digital economy

Law & Economics | Concurrences N° 4-2025 | www.concurrences.com

Christopher Decker

christopher.decker@csis.ox.ac.uk

Research Fellow

University of Oxford - Faculty of Law

ABSTRACT

This paper examines payment models for personal data, comparing “Pay or Consent,” “Pay for my Consent,” and “No Pay and No Consent.” It argues that in one-sided markets, users should be compensated when their data is used beyond service provision, such as being sold or shared. In multisided markets, payments depend on the strength of indirect network effects from targeted advertising. Where these effects are strong, platforms may compensate users beyond providing free access. We briefly outline four approaches to valuing personal data.

I. Introduction

1. Once considered mere exhaust, personal data generated from online interactions is now often referred to as the new oil; a valuable economic resource in a world of “data capitalism.”¹ Nowhere is the value of data more apparent than the exponential growth of large, ad-funded, digital platforms whose business models are based on the collection, combining, processing and sale of data for targeted advertising purposes. In 2023, 98% of Meta’s revenue (USD 131 billion) came from advertising having grown from a mere USD 382,000 in 2004.² Nearly 80% of Alphabet’s revenues come from digital advertisements, with Google’s advertising revenues trebling in value from USD 47 billion in 2014 to USD 146 billion in 2021.³

2. As is the case with other valuable economic resources, questions arise about who does, or should, benefit from the resource. For competition authorities, a focus has been on whether the size of the “data rents” accruing to large ad-funded digital platforms is disproportionate.⁴ Others have focused on how the data rents are allocated and whether the end users who provide the “raw” economic resources are receiving a fair share of the data rents.⁵

3. More generally, there are concerns that the ever-increasing “data power” vested in businesses allows them to constantly surveil individuals and to shape or modify behaviours in ways that support their own interests.⁶ In the US, 81% of adults say they are

concerned about how companies use the data they collect about them.⁷ Courts and competition authorities have also expressed concern about the amount of personal data collected and how it is processed and combined with other data sources to create individual profiles and identifiers to monitor or shape behaviour.⁸

4. Within this context, an emerging debate concerns payments for personal data use. Some argue that end users always have a right to be paid for their personal data and that they are not currently adequately compensated for the valuable data they provide.⁹ Others argue that the value obtained from personal data varies substantially,¹⁰ or that mandating payment for the use of personal data could be destructive of some business models.¹¹

5. Underlying this debate is a fundamental question about when any payment, or other form of compensation, for personal data use should be made. No settled principles on this question exist. However, three potential payment models are emerging.

6. One model involves platform operators requiring users to pay for an online service if they do not consent to their data being used in specified ways

1. See Mayer-Schönberger and Ramge (2018). However, as commentators have noted the data as oil analogy is imperfect and overlooks the fact that, unlike oil, data can be infinite and be re-used.

2. See Evans and Schmalensee (2016) and Meta (2024a).

3. *United States et al. v. Google LLC* (2024).

4. See Aut. conc. (2018); ACCC (2019, 2021); CMA (2020); CNMC (2021).

5. Bergemann et al. (2023).

6. See Zuboff (2019). Tau (2024) raises concerns about the alliance between governments and tech companies.

7. McClain et al. (2023). Similarly, in the UK, it has been estimated that 73% of UK consumers think that companies collect too much personal information. See Quinn (2024).

8. In the US, the FTC (2024) recently observed that “[t]he amount of data collected by large tech companies is simply staggering. (...) They track what we do on and off their platforms, often combining their own information with enormous data sets purchased through the largely unregulated consumer data market” (at i). In *Meta v. Bundeskartellamt*, case C-252/21, the ECJ found that Meta had an ability to process “potentially unlimited data” and that it may create a feeling among users that “his or her private life is being continuously monitored” (para. 118).

9. Bergemann et al. (2023).

10. Iansiti (2022).

11. See *Dr Liza Lovdahl Gormsen v. Meta Platforms Inc., Meta Platforms Ireland Limited, Facebook UK Limited* (2024) at 16.

(typically for personalised advertising). An example is the “Pay or Consent” model proposed by Meta, where users of its social media services (such as Facebook and Instagram) would face a choice between accessing the services for free with personalised ads or paying a monthly subscription for an “ads-free version” of its social networks.¹² The model, which effectively involves users paying *not* to have their personal data used by an online platform for personalised ads if they want to use the online service, has thus far been rejected by both competition authorities and data protection regulators on the basis that it only provides users with a binary choice and does not allow for true consent.¹³

7. An alternative payment model involves users being paid by an online operator if they agree to their personal data being used by the operator in specified ways. This model, which might be termed “Pay for my Consent,” underpins data protection regulations in California, where businesses can pay users for the collection of personal information, and are required to publish a good-faith estimate of the value of the consumer’s data. Compensating users for the use of their personal information is consistent with those who argue that in some cases data may be so valuable for digital platforms that it may be appropriate to pay users for it.¹⁴ However, this view is contested, with some arguing that the assumption that all personal data has value, or that having access to more data always improves a firm’s ability to understand or target advertising to users, is misplaced.¹⁵ On this reasoning, if some personal data has no or minimal value, the argument for automatically compensating users for using their personal data is less clear.¹⁶

8. A third model, which I have termed “No Pay and No Consent,” has been suggested by competition authorities and data protection regulators in the EU.

¹⁷ This model has not been clearly articulated at this point but would seem to require certain large online platforms that wish to introduce a “Pay or Consent” model to also offer an additional free service to end users who do not consent to behavioural or personalised advertising. This might involve providing a free service to end users, which is funded by advertising that is less targeted and thus requires less processing of personal data. In November 2024, Meta launched a “*less personalized ads*” option along these lines, which would allow users to continue to use Facebook and Instagram for free and the ability to choose to see “*less personalized ads*.”¹⁸

9. This paper considers the merits of the three payment models described above. Section II provides an overview of relevant legal and economic context, while Section III sets out principles relevant to the question of when payments for personal data use may be appropriate in different settings. It also briefly considers different approaches to valuing or putting a price on data.

II. The economic and legal context

1. Personal data as an economic resource

10. Personal data generates value as an economic resource in three ways. First, firms that operate online, including large digital platforms as well as firms of all sizes and sectors of the economy, can use personal data to better understand the profile of those who visit their website and consume their goods or services. The categories of information collected can be extensive. Table 1 presents an example of the types of personal information collected by the US retailer Walmart when interacting with its customers

12. The original monthly subscription was EUR 12.99, although this has since been reduced. See Meta (2024b)

13. See Eur. Comm. (2024). The EDPB (2024) concludes that while “Pay or Consent” models will not inevitably be excluded, they will require better justification, transparency and granularity of options for large platforms.

14. See Tirole (2020) at 3, who notes “*the theoretical possibility that a zero price may still be too high, as data are extremely valuable to platforms (...) (that is, the flow of payments [should] be toward consumers).*”

15. Iansiti (2022) argues that the value of data to online advertising can be significantly less than is often assumed in regulatory discussions. He notes that while highly time-dependent data (e.g. geolocation information for targeting consumers) can be quite valuable for advertisers, it can have a “*rapidly decaying utility.*” He also refers to studies where additional data such as demographics and ad exposure data provided essentially no performance improvements.

16. Even those who advocate that users should be paid for data recognise that the value of data can vary significantly, and that the marginal value to a platform of an individual user’s personal data is small and does not change the price it can levy for advertising. See Bergemann et al. (2023).

17. EDPB (2024) and Eur. Comm. (2024).

18. According to Meta (2024b), “[t]his *less personalized ads* option relies on less data, so we’ll show ads based only on context – what a person sees in a particular session on Facebook and Instagram – and a minimal set of data points including a person’s age, location, gender, and how a person engages with ads.”

in different contexts.

11. Personal data can be used to make inferences and predictions about an individual user's personal needs, opinions and preferences, their creditworthiness, what products and services they might consume and their willingness to pay for those products.¹⁹ Online firms often supplement their own data collection activities with additional data acquired from third-party sources to improve the quality and personalisation of services.

Table 1. Categories of personal information collected

Identifiers	Personal identifiers, such as name, telephone number, physical address, email address, national identification numbers, driver's license numbers, and signatures
Device Information and Online Activity	Device and online identifiers, keystroke patterns indicative of human or bot website/app usage, mobile and web network activity and related information (such as Mac address, IP address, cookie IDs, browser activity, and other information associated with your browsing history), and social media information
Commercial Information	Purchase and transaction history information (such as products or services you have purchased, rented, or returned), health- and safety-related information, product testimonials, travel and vacation information, and competition entries
Communications	Communication details (such as the content of emails, text messages, or other communications), call logs, and calendar information where Walmart is a party to the exchange
Demographic Information	Demographic information, such as age (including information about children under the age of 13 with respect to certain purchases and services (e.g., tobacco purchases), gender, citizenship, ethnicity, date of birth, family or marital status, household income, education, professional and employment information, family health, number of children, number of cars owned, and software or virtual assets owned
Financial Information	Financial information, such as credit or debit card numbers, financial account numbers, and claims information
Biometric Information	Biometric information, such as voice prints, imagery of the iris or retina, face geometry, and palm prints or fingerprints
Geolocation	Location information, such as geolocation information
Sensory Information	Audio, visual information, and other sensory information such as photographs and audio and video recordings
Background Information	Background and criminal information, such as background checks and criminal convictions
Inferences	Individual preferences and characteristics, such as inferences related to shopping patterns and behaviors, intelligence, and aptitudes
Sensitive Personal Information	Government-issued identifiers (such as social security, driver's license, state identification card, or passport number), account log-in and financial information (such as payment card details), and precise geolocation

Source: Walmart (2024)

12. A second way personal data generates value is when it is sold or shared with third parties.²⁰ This can include selling or sharing information about an individual's account and history, personal details, purchase transactions, etc. Data traders and brokers offer access to vast amounts of information on individuals. In 2014, one of the world's largest data brokers, Acxiom, claimed to have, on average, 1,500 pieces of information on more than 200 million Americans at that time.²¹ This has undoubtedly increased with the exponential growth in data,²² and some data brokers now claim to have over 2.4 billion data records and over 293 billion real-time data signals.²³

13. The third way personal data generates value is for social media or other digital platforms that are funded through selling space to businesses for targeted or behavioural digital advertising.²⁴ Unlike conventional advertising, digital advertising allows ads to be highly personalised or tailored to an individual user based on their profile, location or past behaviour (i.e. browsing or purchase history). This means that users of the same webpage or app can see different ads (known as impressions) that are personalised to them.²⁵ The technology that facilitates the sale and purchase of digital advertising space on websites and apps is known as AdTech. Critically, the buying and selling of impressions in the so-called AdTech stack typically takes place in the fraction of a second between when a user clicks to open a webpage and the webpage content opening.²⁶

14. Many large digital platforms (such as Google, Meta, and Microsoft) are highly integrated throughout the AdTech stack, giving them an ability to access, combine and analyse personal data from a disparate set of sources. In addition, digital platforms that operate in multiple markets (super platforms) can combine personal data about a specific user across platforms and supplement information on users from third-party websites accessed using an operating system owned by the operator.²⁷ This provides them

19. See OECD (2019); ACCC (2019); Zuboff (2019); CMA (2020); FTC (2024).

20. In some jurisdictions, such as the EU and California, online operators need user consent before doing so.

21. Kroft (2014).

22. Some reports suggest that we generate 2.5 quintillion bytes of data each day. See Marr (2018).

23. Redmob (2024).

24. In 2023, Meta earned USD 131 billion by displaying ad products on Facebook, Instagram, Messenger, and third-party mobile applications. In the same year, Google's earned USD 206 billion in revenues from delivering advertising on; Google Search and other properties; search distribution partners who use Google.com as default search; other Google owned and operated properties (Gmail, Google Maps and Google Play); and You Tube. See Alphabet Inc. (2024) and Meta (2024c).

25. As Calvano and Polo (2021) observe, "new technologies allow advertisers to 'target' audiences in a number of dimensions: demographics, physical location, time of the day, personal tastes, browsing history and so on. (. . .) Targeting means that competition is scaled at the individual level."

26. AdTech stack participants collect data using different methods and tools, including the placing of cookies on a device, JavaScript tags, web pixels, device fingerprinting techniques and other tracking technologies.

27. The CMA (2020) found that Google collected a "vast amount of user data from three main sources: from its user-facing services (it provides over 50 such services, including search and Gmail); from mobile devices running Android, Google's operating system; and from the analytical technology they place on third-party sites and apps (known as tags). Facebook gathers user data from the three main services it provides in the UK (Facebook, Instagram and WhatsApp) and from Facebook analytics technology placed on third-party sites (known as pixels)". Similarly, the ACCC (2019) notes that Google obtains data from its own sites, but also obtains data from third-party sites when a consumer uses a device with an Android operating system or a Chrome browser to access a third-party website. This allows it to offer advertisers data about sales of search and display inventory on its own websites and data about sales of search and display inventory on third-

with an even better ability to offer advertisers highly targeted, personalised and timely impressions.²⁸

2. Laws that protect personal data

15. Personal data is, of course, much more than just an economic resource. Nor is it only used for advertising. It can also be used for a range of profiling and targeting purposes. Accordingly, a range of laws restrict how firms and other undertakings can use personal data.²⁹ These include data protection laws, laws relating to digital markets and services, and competition law. Although individuals have certain rights to protect their privacy and personal data under these laws, they do not “own” their personal data, and it is not a property right that can be transferred.

2.1 Data protection laws

16. Data protection laws aim to strike a balance between the privacy rights of the individual (data subjects) and the ability of firms and other undertakings (data controllers) to process and share personal data.³⁰ The EU’s General Data Protection Regulation (GDPR) permits enterprises to process personal data only where there is a lawful basis to do so (such as when a data subject gives their consent). It also requires transparency to data subjects as to how their data will be used and with whom it will be shared. Where the legal basis for processing relied on is “consent”, such consent must be freely given, informed and unambiguous.³¹ In determining

party websites.

28. As the court observed in *United States et al. v. Google LLC* (2024) at 230: “The more precisely targeted an ad, the greater likelihood that it will be clicked, which translates into higher revenues that Google uses to make larger revenue share payments.”

29. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Art. 12), the European Convention of Human Rights (Art. 8) and the European Charter of Fundamental Rights (Art. 7). In common law jurisdictions, tort provisions relating to the misuse of private information further enshrine an individual’s right to a reasonable expectation of privacy.

30. Separate laws concern how personal data is collected from users, such as the deployment of cookies or similar technologies (such as fingerprint technologies).

31. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), OJ L 119, 4.5.2016, p. 1, Art. 4(11).

whether consent is “freely given,” it is relevant to consider whether the provision of a service is made conditional on agreeing to the processing of data that is not necessary for the provision of the service. As discussed later, this requirement has impacted EU decisions looking at the “Pay or Consent” model.

17. The Californian Consumer Privacy Act (CCPA) gives consumers a right to know about the information that certain online businesses collect about them and how it is used and shared. It also provides a “right to opt-out of the sale or sharing of their personal information.”³² However, businesses can charge consumers different prices, or offer different levels of service, if the difference is “reasonably related to the value provided to the business by the consumer’s data.”

18. In other words, under the CCPA, businesses can offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information.

³³ Businesses are required to publish a financial incentive notice, which, among other things, explains how the financial incentive is “reasonably related to the value of the consumer’s data, including: (. . .) [a] good-faith estimate of the value of the consumer’s data (. . .) and (. . .) [a] description of the method(s) the business used to calculate the value of the consumer’s data.”³⁴

2.2 Laws relating to digital markets and services

19. In addition to data protection laws, some jurisdictions have introduced laws specifically targeted at digital markets that further restrict the use of personal data by designated firms. The EU Digital Markets Act (DMA) requires that designated large digital platforms (“gatekeepers”) seek users’ consent for combining their personal data between designated core platform services and other services, and critically, if users do not provide such consent, it requires that they be offered a less personalised but equivalent alternative.³⁵

32. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199, § 1798.125.

33. Ibid., § 1798.125(b)(1).

34. Cal. Code Regs. tit. 11, § 7016(d)(5)(A) and (B) (2022) (formerly numbered as § 999.307(b)).

20. Similarly, the EU's Digital Services Act ³⁶ requires that all online platforms be transparent to users about why an ad specifically targets them. It prohibits profiling that rests on special categories of personal data (e.g. ethnicity, political views or sexual orientation) and the use of behavioural targeted advertising for minors.

2.3 Competition law

21. Competition law can also be used to address concerns about the collection, processing and sharing of data by large digital platforms. ³⁷ The most prominent example is the Bundeskartellamt's *Facebook* decision, which found that Meta abused its dominant position by requiring users to accept terms that allowed Facebook to collect "*off-Facebook data*" for the purposes of creating personalised advertising messages for Facebook users. ³⁸ On appeal, the European Court of Justice (ECJ) ruled that users must be free to refuse individually to give their consent to particular data processing operations without being obliged to refrain entirely from using Facebook. In a critical passage, the ECJ said that users should be "*offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.*" ³⁹

22. Following this statement and the introduction of the DMA, Meta announced in November 2023 that it would introduce a "Pay or Consent" model for using its social networks (Facebook, Instagram). Users would be offered a subscription to an ad-free version of its social networks for a cost of EUR 12.99 per month, or the ability to access the social networks free-of-charge with personalised ads. ⁴⁰

23. In July 2024, the European Commission issued a preliminary decision that Meta's "Pay or Consent" model was incompatible with the DMA requirements. This was because it does not allow users to opt for a service that uses less personal data but is otherwise equivalent to the personalised ad service, and did not allow users to exercise their right to freely consent to their personal data being combined. ⁴¹

24. Although the Commission's preliminary decision was made under the DMA, it is consistent with an earlier report of the European Data Protection Board (EDPB), which considered the merits of the "Pay or Consent" approach more generally under the GDPR. ⁴² The EDPB indicated that, in most cases involving large digital platforms, confronting users with a binary choice between consenting to the processing of bundled personal data for behavioural advertising purposes or paying a fee was unlikely to satisfy the requirements of valid consent. The EDPB suggested that platforms must consider their ability to provide an "*equivalent alternative that does not entail the payment of a fee,*" ⁴³ including through consideration of advertising that involves less (or no) processing of personal data.

25. In the UK, a collective action against Facebook currently before the Competition Appeal Tribunal (CAT) also involves a claim that Facebook abused its dominant position by making users a "*take it or leave it offer*" requiring them to agree to the collection and processing of "*off-Facebook data.*" However, the issue is being considered in a different way to how it was assessed by the Bundeskartellamt and the ECJ.

26. The claimants in these proceedings argue that Facebook users were not adequately compensated for the economic value of their off-Facebook data, or put differently, they received an "*unfairly low zero-price in return for their Off-Facebook data.*" ⁴⁴ In other words, they contend that users should have been paid by Facebook for providing their personal data. However, in its preliminary judgment, the CAT

35. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act or DMA), OJ L 265, 12.10.2022, p. 1, Art. 5(2) and Recital 36. Recital 37 further clarifies that "[t]he less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service."

36. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act or DSA), OJ L 277, 27.10.2022, p. 1.

37. See Buiten (2021); OECD (2024).

38. This included sensitive and non-sensitive data about a user's visits to third-party webpages and apps, as well as data concerning the use of other online services belonging to the Meta group, such as Instagram and WhatsApp.

39. *Meta v. Bundeskartellamt*, case C-252/21, paras. 150 and 151.

40. See Meta (2024b), which refers to the original press release of 30 October 2023.

41. Eur. Comm. (2024).

42. EDPB (2024).

43. Ibid. at 3.

44. *Dr Liza Lovdahl Gormsen v. Meta Platforms Inc., Meta Platforms Ireland Limited, Facebook UK Limited* (2024), para. 28.

cautioned against this approach, noting that it could lead to a situation where “[u]sers will be able to charge a price for such data going beyond simply the ‘free’ use of Facebook; and that the effective imposition of such a price would be destructive of Meta’s business model.”⁴⁵

III. Principles for when payments for personal data may be appropriate

27. The discussion in Section II raises a wider question about when payments for personal data use are appropriate. In this part, we seek to establish some guiding principles relevant to this question by distinguishing between the different market settings where personal data is collected and used.

1. Payments for personal data in “one-sided” markets

28. Most online firms that sell retail products and services (e.g. sellers of running shoes) operate in a one-sided or “single-sided” market, meaning that the customer relationship is entirely controlled by the online provider. The online retailer directly deals with its input suppliers to manufacture a product that it then sells to customers. They are not “platforms” that match sellers directly with customers (like an online marketplace) or users with other users (such as social media platforms).

29. However, as part of a transaction, online retailers increasingly request customers’ consent to using their personal data for purposes beyond those needed to complete the transaction or purchase (see, for example, Table 1 above). As described in section II.1 above, this may be for internal purposes to better understand their customers, or the data may be collected for the purposes of selling or sharing with third parties.

30. In this one-sided setting, there is a clear separation between the value of the product being

offered online (e.g. the running shoes) and the value of the personal data. Where the online retailer obtains an additional benefit from the customer consenting to share their personal data for other purposes, such as through selling or sharing of the data with third parties, there is an in-principle argument for the online provider to share some of this additional benefit with the customer. In other words, the online provider should arguably “pay” or compensate customers in the form of financial incentives for their additional uses of the personal data.⁴⁶

2. Payments for personal data in “multisided” markets

31. Establishing when payments for personal data should occur is more complicated when the product is an online service (or group of services) provided by a digital platform in a multi-sided setting. A multisided market is one where there is an interdependence between different types of user groups and network effects. User groups are interdependent in multisided markets because the demand for a service by one user group is conditioned by the demand for the use of the service by other user groups.

32. Ad-funded digital platforms match one group of users (end users of the platform) with other groups of users (e.g. advertisers). The financial performance and sustainability of the platform depend on how successful the operator is in offering each group incentives to use the platform.⁴⁷ For ad-funded digital platforms, this has typically involved offering end users access to a core online service offered by the platform for no direct monetary payment (i.e. for “free”) provided the user consents to their personal data being used for purposes beyond those needed to provide the online service (typically the data is combined and monetised in the AdTech stack to facilitate targeted advertising).

33. The online service and personal data are thus inextricably linked for ad-funded digital platforms.⁴⁸ The “input” that finances the platform is personal

45. Ibid., para. 25(1).

46. This may take the form of direct payments or, more commonly, financial incentives such as membership of a loyalty club that provides discounts on purchases or other benefits.

47. This logic is succinctly captured in *United States et al. v. Google LLC* (2024) at 2: “More users mean more advertisers, and more advertisers mean more revenues.” See generally, Evans and Schmalensee (2016).

data: they acquire it from users by offering a core online service for “free” and then use this data to allow advertisers to send targeted and relevant impressions to an individual end user almost instantly. The critical question is when users should be “paid” or compensated for the use of their data over and above receiving the online service for free. The answer to this question depends, in part, on the magnitude of any indirect network effects of using personal data for targeted advertising.

34. Network effects arise where the benefits to one user of a network depend on the number of other users that are connected to, or utilise, the network. They can be positive or negative, and direct or indirect.⁴⁹ For ad-funded digital platforms, indirect network effects arise when the number of end users (and, critically, the type, quality and granularity of personal information they provide) increases (or decreases) the value of using the platform to another type of user group (advertisers).

35. When setting the “price” and non-price terms that each group should face, an ad-funded platform operator must therefore consider not only how the terms set for end users will affect the demand for that user group (direct network effects),⁵⁰ but also how any changes in resultant demand will affect the attractiveness of the platform to other user groups such as advertisers (indirect network effects).⁵¹ It is within this context that the question of payments for personal data must be considered.

36. To begin, consider the example where there are moderate indirect network effects such that the benefit that the platform obtains from using the personal data in the AdTech stack or elsewhere is exactly equal to the costs (including a normal return

on investment) of providing the online service to end users. For example, the monthly costs of operating a social media platform might be EUR 12 per user, while the monthly revenues that the social media operator obtains from using personal data in the AdTech stack also works out at approximately EUR 12 per user. In this simplistic example, there is arguably no need for the platform operator to directly pay or compensate end users if the online service is provided to the user for free. This is because advertisers are fully subsidising the “free” use of the online service by end users.

37. In contrast, consider the situation where there are strong indirect network effects such that the value that the platform obtains from using the personal data in the AdTech stack or elsewhere is substantially greater than the costs (including a normal return on investment) of providing the online service to end users. For example, the monthly revenues that the platform operator obtains from using personal data might be EUR 24 per user, while the monthly costs (again including a normal profit) of operating the digital platform might be EUR 12 per user. The financial benefit that the digital platform operator obtains from using personal data is therefore double the costs of providing the service to end users. In this case, there is arguably a case for adjusting the pricing structure such that end users receive additional compensation for providing personal data over and above just being able to use the online product for “free.” This might involve end users being compensated in the form of a direct monetary payment or a payment in kind (i.e. discounts or other benefits) up to an annual amount of EUR 144 a year as well as being able to access the online service for free.

38. The “Pay for my Consent” model, which would involve digital platforms paying end users for using their personal data, reflects this logic. It assumes that personal data generates significant positive indirect network effects in the form of advertising revenues and that the appropriate level of compensation to end users is greater than just receiving an online service for free.

39. A third scenario is where there are weak or negligible indirect network effects of using personal data for targeted advertising such that the benefits of personal data to a platform operator are lower than the costs of providing an online service to end users. This may be because the type, timeliness and

48. This contrasts with a one-sided market where the transaction involving the exchange of the online product (e.g. running shoes) happens independently of the collection of personal data, and the online provider does not directly rely on the revenues generated from the personal data to finance its business.

49. Belleflamme and Peitz (2021) refer generally to “*attraction spirals*” (for positive indirect network effects) and “*attraction/repulsion pendulum*” (for negative indirect network effects that generate positive effects for one group but negative effects for another group).

50. Direct network effects are important for social media platforms, which need more users to connect with one another on the same side, as well as for search engines, which need more user queries to improve their algorithms, which in turn attracts more users to their search engine.

51. Belleflamme and Peitz (2021) discuss more generally the different strategies that platforms use, including a “*divide-and-conquer strategy*,” which involves subsidising the user group that exerts the stronger network effects.

granularity of the personal data collected are not useful to advertisers. In these circumstances, in addition to providing their personal data when using the online service, users might be required to pay an additional amount to use the online service. This type of situation might arise for smaller, or entrant, digital platforms that earn some advertising revenues but are not well integrated in the AdTech stack or have difficulty attracting a large base of end users (and therefore collecting sufficient personal data to be attractive to advertisers as a platform to place targeted impressions).

40. This is effectively a subscription-type approach where end users no longer receive the online service for free. In broad terms, this is the logic behind the “Pay or Consent” model, which assumes that end users that do not consent to sharing their personal data will no longer generate significant positive indirect network effects in the form of advertising revenues and therefore should pay to cover some or all the costs of using the online service.

3. The “No pay and No consent” model

41. As discussed above, the EDPB and the European Commission have found that a binary “Pay or Consent” model can be incompatible with the GDPR and the DMA in some markets and are requiring large platforms to consider offering users other options, including, where reasonable, a “No pay and No consent” option.⁵² This may allow users to access an online service free of charge and not be required to consent to their personal data being used for the purposes of targeted personalised (behavioural) advertising.

42. Given its attributes, the “No pay and No consent” model would likely be attractive to many end users,⁵³ except those end users who value receiving targeted and personalised advertisements. This might reduce the number of advertisers that use the platform, or the amounts that they will be willing to pay to advertise on the platform because they will no longer be able to send targeted personalised impressions.⁵⁴

43. The equilibrium effects of this model will therefore depend on the scale of any indirect network effects attached to the use of personal data for targeted personalised advertising. Where indirect network effects attached to personal data are very strong, and advertisers choose to no longer use the platform, or significantly reduce the amounts they are willing to pay for advertising, this could substantially reduce the revenues the platform operator receives from the advertising side of the market. Conversely, where the indirect network effects are moderate or negligible, it may be the case that the “No pay and No consent” model does not significantly impact a platform’s revenues or sustainability. This may be because the advertisers continue to advertise on the platform in a less targeted and personalised way. For example, they may continue to use the platform to place contextual impressions rather than targeted personalised impressions.

4. How to value personal data?

44. An important thread running through this paper is how to place a value on personal data. This is central to any assessment of whether the compensation offered, or price paid, for the use of such data represents “fair” or reasonable compensation for that data’s value.

45. The question of how to value or put a price on personal data is complex and beyond the scope of this short paper. However, we note in passing that there are, in principle, four potential ways of approaching this evaluation exercise.

46. A first approach is to focus on the costs of collecting and processing data. Given its unique characteristics as a product (i.e. non-excludable and non-rivalrous), and the fact that there can be a major disconnect between the value obtained from data and the costs associated with collecting, processing and sharing it, a standard cost-based “utility-style” approach does not seem an appropriate way to place a value on personal data.

47. A second approach is to assess the value of data in terms of the benefits it provides to an online

52. EDPB (2024) refers to this as a “Free Alternative Without Behavioural Advertising.”

53. This is consistent with studies such as Leszczynska and Baltag (2024), who find that most individuals are hesitant to share personal data for any form of personalisation.

54. Fang and Kawaguchi (2025) find that browser prohibitions on advertisers’ ability to track user information and target potential customers (so-called retargeting) reduced advertiser bid valuations by more than 60%. This is because such prohibitions significantly limited advertisers’ access to user information and their ability to effectively target consumers.

provider or digital platform. As described above, this is the approach in California, where businesses may offer payments, or a reduced price for goods or services, to a consumer if that payment or difference in price is reasonably related to the value provided to the business by the consumer's data. This approach also underpins Meta's "Pay or Consent" proposal. In that case, the proposed price that non-consenting users would pay for the online service might be seen as the "shadow" value of the benefit of personal data to Meta.

48. If online operators are allowed to determine the value, and the amount of any resultant payment, for personal data, then there is arguably a strong case for some form of economic regulatory oversight. Such oversight would be particularly relevant for large digital platforms, but it might even need to apply to smaller online operators. In California, for example, significant variations exist in the approaches adopted by businesses to value data and the compensation levels offered to consumers. Some businesses estimate a precise monetary value of personal information;⁵⁵ others base it on the cost of providing the financial incentive, or on the anticipated revenue from the personal information less anticipated expenses;⁵⁶ while the valuation approach used by other firms is ambiguous and based on several factors.⁵⁷

49. A third valuation approach is to focus on the value of personal data to the user. Put differently, the focus would be on how much a user would be willing to "sell" their personal data if such a market existed. Various surveys have sought to provide such valuations and have provided a wide range of estimates depending on the type of data that is accessed and how sensitive it is, and the purposes to which the data will be put.⁵⁸

50. Some commentators have proposed that data intermediaries be established by regulation to overcome the practical problem of individuals negotiating with online providers for payments every time their personal data is used.⁵⁹ Such

intermediaries would sit between consumers and firms that wish to use their personal information and would be empowered to monetise users' personal data and permit other uses in accordance with user instructions. The actual payments that individual consumers receive for their personal data would, under this proposal, be the result of competition between intermediaries.

51. A final data valuation approach might estimate the value of personal data by reference to the amounts exchanged when it is sold by data brokers or traders. There is an active market in data trading, and some reports estimate that the market is worth between USD 200 billion and USD 300 billion, with up to 4,000 data brokering firms worldwide.⁶⁰ While this provides a market-based valuation of personal data, there are several challenges in inferring the value of personal data given the current market structure for data trading, including the fact that traders tend to sell highly aggregated datasets that combine data from various sources.

IV. Concluding remarks

52. The aim of this paper is to contribute to the debate about payments for personal data by providing an overview of relevant economic and legal context, and to establish some general principles about when payments for personal data use may be appropriate in different market settings. It also considered the merits of three emerging payment models: "Pay or Consent," "Pay for my Consent," and "No pay and No consent."

53. While the idea that end users could be paid, or compensated, for the use of their personal data might seem far-fetched and impractical, there are several reasons to believe that payments associated with personal data will become more common in the future. First, competition authorities and courts around the world are increasingly concerned that large digital platforms are earning excessive returns from using data to sell advertising on their platforms. This may lead to policies requiring that some

55. For example, General Motors (2024) estimates the value of consumer data at USD 1.09; Marriott (2024) at USD 0.54, while North Face (2024) values consumer data at USD 33.

56. Simon & Schuster (2024) and Adquization (2024).

57. See inKind (2024); MGA (2024)

58. See Benndorf and Normann (2017); Skatova et al. (2023); Winegar and Sunstein (2019).

59. Bergemann et al. (2023).

60. Boutin (2016) and Kaspersky (2024).

proportion of the large data rents derived from advertising are shared with end users.⁶¹

54. Second, there is growing consumer and citizen concern about privacy and profiling and, separately, increasing awareness that personal data has value. Across the world, many citizens feel as though their lives are being increasingly monitored and surveilled

61. As the CMA (2020) market study concluded, “*the profitability of both Google and Facebook has been well above what is required to reward investors with a fair return for many years. (. . .) We would expect these excess profits to be shared more freely with consumers in a more competitive market*” (para. 12).

by online providers, and this is fuelling interest in ways of providing users with more choice about the types and amount of data that is being collected and shared online.

55. Finally, it is important to recognise that the general principle of “paying” or compensating users for their personal data already exists in some jurisdictions (e.g. California). There is also increasing academic and policy interest in potential institutions (such as data intermediaries) that could facilitate the ability of individuals to monetise and be compensated for the use of their personal data.

Concurrences is a monthly journal covering all aspects of European Union and national competition laws. It provides indepth analysis through academic articles, practical law notes, and case comments.

Forewords

Jacques Attali, Laurent Benzoni, Elie Cohen, Eleanor Fox, Marie-Anne Frison-Roche, Thierry Guimbaud, Douglas H. Ginsburg, Frédéric Jenny, Roch-Olivier Maistre, Mario Monti, Fiona M. Scott-Morton, Jean Pisani Ferry, Jacques Steenberg, Denis Waelbroeck, Marc van der Woude...

Interviews

Sir Christopher Bellamy, Sarah Cardell Eshien Chong, Lord David Currie, Thierry Dahan, John Fingleton, Damien Gérard, Olivier Guersent, François Hollande, Herbert Hovenkamp, William Kovacic, Neelie Kroes, Christine Lagarde, Johannes Laitenberger, Emmanuel Macron, Pierre Régibeau, Tommaso Valletti, Christine Varney, Margrethe Vestager...

Insights

Jean Philippe Arroyo, Ian Forrester, Calvin Goldman, Ioannis Kokkoris, Petros C. Mavroidis, Frank Montag, John Pecman, Irving Scher, Andreas Schwab, Patrice Spinosi, John Taladay...

On-Topics

Jacques Barrot, Jean-François Bellis, David Bosco, Murielle Chagny, Damien Géradin, Calvin Goldman, Assimakis Komninou, Christophe Lemaire, Pierre Moscovici, Damien Neven, Jorge Padilla, Emil Paulis, Andreas Schwab, Richard Whish...

Articles

Rafael Amaro, Luca Arnaudo, Mor Bakhoun, Zohra Boumedhel, Vincent Bridoux, Guy Canivet, Emmanuel Combe, Guillaume Fabre, Daniel Fasquelle, Georgios Gryllos, Nathalie Homobono, Laurence Idot, Charles Jarrosson, Bruno Lasserre, Ioannis Lianos, Luc Peeperkorn, Nicolas Petit, Catherine Prieto, Joseph Vogel, Wouter Wils...

Legal Practice

Legal privilege, Cartel Profiles in the EU, Competitive risks in the pharmaceutical sector, Digital Markets Acts and competition, EU foreign investment control, Antitrust and Artificial Intelligence, Failing firm defence, Labor market competition, Merger control in digital markets.

International

Belgium, Brazil, Canada, China, Germany, Hong Kong, India, Japan, Luxembourg, Sweden, Switzerland, USA...

Law & Economics

Georg Clemens, Pierre Y. Cremieux, Adriaan Dierx, Fabienne Ilzkovitz, Gregor Langus, Vilen Lipatov, Patricia Lorenzo, Damien Neven, Georgios Petropoulos, Edward Snyder, Nadine Watson, Mutlu Özcan...

Chronicles

ANTICOMPETITIVE PRACTICES

Anne-Sophie Choné Grimaldi, Michel Debroux, Marie Hindré

UNILATERAL PRACTICES

Marie Cartapanis, Frédéric Marty, Nicolas Zacharie

UNFAIR PRACTICES

François-Xavier Awatar, Frédéric Buy, Valérie Durand, Jean-Louis Fourgoux, Marie-Claude Mitchell

DISTRIBUTION

Nicolas Eréséo, Nicolas Ferrier, Anne-Cécile Martin, Philippe Vann

MERGERS

Franck Audran, Olivier Billard, Etienne Chantrel, Eric Paroche, Igor Simic, David Tayar, Simon Vande Walle

STATE AID

Jacques Derenne, Francesco Martucci, Bruno Stromsky, Raphaël Vuitton

PROCEDURES

Alexandre Lacresse, Christophe Lemaire, Barbara Monti

REGULATORY

Orion Berg, Guillaume Dezobry, Emmanuel Guillaume, Sébastien Martin, Francesco Martucci

TENDERS

Bertrand du Marais, Arnaud Sée, Fabien Tesson

PUBLIC ENFORCEMENT

Virginie Coursière-Pluntz, Jean-Philippe Kovar, Aurore Laget-Annamayer, Jérémy Martinez, Francesco Martucci

INTERNATIONAL

Walid Chaiehloudj, Rafael Allendesalazar, Laurence Nicolas-Vullierme, Silvia Pietrini

Books

Under the direction of Catherine Prieto

Review

François Aubin, Maud Boukhris, Lucile Chneiweiss, Lucien Frys

> Concurrences + *Quote upon request*

Unlimited access to the entire database

- 12 issues of the Concurrences Review with 15,000 archives
- 45 issues of the e-Competitions Bulletin with 30,000 archives
- 75+ eBooks and printed versions of books published during your subscription
- 650+ conference materials: summaries, transcripts, audio files, PPT presentations

Premium services

- Access to the ConcurrencesAi tool to facilitate your legal research
- Option to download PDF versions of all articles and documents
- Named user access and access via IP addresses

> Concurrences Select *Quote upon request*

- 12 issues of the Concurrences Review with 15,000 archives
- 45 issues of the e-Competitions Bulletin with 30,000 archives
- 650+ conference materials: summaries, transcripts, audio files, PPT presentations
- Named user access and access via IP addresses

> Concurrences Basic *Quote upon request*

- 12 issues of the Concurrences Review with 15,000 archives
- 45 issues of the e-Competitions Bulletin with 30,000 archives
- Named user access

For any additional information or to request a customized quote, please contact us at **subscriptions@concurrences.com**. A member of our sales team will be delighted to respond within 24 hours.

You can also reach us directly by phone at **+33 6 95 25 93 33**.

To enjoy a free trial,
please **[click on this link](#)**.