Defining Privacy in the Competition Law Sphere

Arletta Gorecka

University of Strathclyde, Glasgow, Scotland

Email: Arletta.gorecka@strath.ac.uk

Defining Privacy in the Competition Law Sphere

The unprecedented magnitude of data collection could raise challenges for both society and legislation, as it has emerged that personal data is seen as a tradable commodity, placing companies in a position where the data helps them to achieve a stronger position in a market. Yet, the debate is missing a crucial link—the definition of privacy. It has been already widely noted that privacy invasions and data breaches are increasingly presenting a danger to society. In theory, some of the competition enforcements might be capable of considering the increased consequences of commercial processing or collection of personal data. Hence, the price of the privacy is difficult to be ascertained. In essence, this article is about the impact of privacy in competition law sphere, and its features of division and connection, signifying developments, and highlights difficulties in anticipating the new structural form of the industry. This article discusses the understanding of the new data-based industry, and provides an overview of the key legal developments in relation to competition law and privacy, placing an emphasis on Facebook case (2019). The debate emphasises on potential connections and divisions in relation to defining a relationship between competition law and privacy, and discusses the multi-dimensional nature of privacy protectionism.

Introduction

The debate on the intersection between competition law and privacy constitutes a major challenge for the existing competition law framework. The notion of privacy has achieved extensive attention from academics and adjudicators, indicating its dynamic nature (EDPS, 2016). Online platforms offer a high quality of digital services and products to users without imposing any monetary price. However, they keep obtaining revenue from the advertisement-based business models, based on the collection and processing of data. Examples of such networks are extensive and cover platforms including Facebook, YouTube or Google.

The question as to what privacy means within the development of competition law remains to be discussed. The nature of privacy appears to indicate its multidimensional nature, forming an element of a free and democratic society. In many respects, the sole discussion should not be based on an argument regarding the value of privacy, since its value could depend on a particular case, but on the assessment behaviour of undertakings acquiring data, and its effect on competition. Certainly, the angle of the debate demonstrates the existence of two groups of schools, which connect and divide the meaning on the privacy within the competition law debate.

To begin the discourse on the dynamic nature of data within the changing commercial society, this article discusses the understanding of the new data-based industry. In essence, this article is about the impact of privacy in competition law sphere, and its features of division and connection, signifying developments, and highlights difficulties in anticipating the new structural form of the industry.

The article will begin with the basic discussion describing legal backgrounds of both competition law and data protection law within the doctrinal context. Such discussion is necessary to demonstrate the potential connections and divisions of these legal areas.

Subsequently, the debate moves to discuss the German Facebook case, which, arguably, could be seen as the cornerstone of this debate. The case is important to define various connections and divisions of the debate on the nature of privacy from competition law perspective. It demonstrates the tension and serves as a bridge for understanding how privacy and competition law could be interconnected. Once the legal foundations are discussed, the emphasis is placed on definition of privacy for competition purposes, acknowledging its legal and societal importance. This would allow demonstration of the connection and division of the two different, however, arguably, interlinked areas of law.

Before discussing these aspects in detail several limitations should be mentioned. The article does not attempt to determine the objective of competition law in the deeply doctrinal basis. Instead, the scope of this article is limited, as the discussion covers the extent that applies to the digital economy's free high technology industry.

Legal Background: Discussing Competition Law and Data Protection Laws of the EU

EU Competition Law

EU competition law pursues a multitude of different aims that include the protection for market structures, economic freedom, consumer welfare and the promotion of efficiency. Article 101-106 TFEU (2008) sets out the rules on competition law, which aim at prevention or distortion of competition, or abuse of a dominant position. EU competition law applies to any 'economic activity 'that might 'affect trade between the Member States '(Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, 2004). The emphasis is placed on Article 102 TFEU (2008), which prohibits the abuse of a dominating position in a relevant market.

Article 102 TFEU (2008) could apply to the anticompetitive actions of online platforms, which operate on the data acquisition. Yet, a mere dominance in a relevant market is not prohibited. Article 102 TFEU only acts as a sword in the instances of a detected abuse of dominant position. An abuse under 102 TFEU is understood as taking forms of exclusionary abuse and exploitative abuse (Commission guidance, 2009).

The exploitative conduct refers to an action which harms consumers (in most cases the victims were companies, and not end consumers) and includes an application of excessive prices or unfair discrimination (Hubert, Combet, 2011). According to *United Brands* (1972), the Commission, to determine whether an action amounted to an exploitative abuse, is required to determine whether: (i) the price is unfair in itself or unfair whether compared with competing products, and whether (ii) the profit margin amount is excessive by comparing product cost with price. The exclusionary conducts refer to the abuse by which the market structure is damaged (Commission Guidance, 2009, paras 5, 19), and includes specific forms of tying, bundling, refusal to supply, market squeeze, and predation (Commission Guidance, 2009). The actions of exclusionary abuse are deemed to be harmful to consumers and have an impact on consumer welfare.

Furthermore, competition law also applies to mergers, which by its nature bring structural changes to the market. Merger control aims at regulating undertakings activity, accounting its effect on competition, taking into account the factors like including its interest on consumers (Commission Guidance, 2009). Mergers tend to impact the structure of a relevant market, and often goes beyond the national borders of a Member State. The nature of the merger review falls within the scope of regulation and is appraised by the Commission.

EU Data Protection Law

Article 16 TFEU serves as a basis for the EU data protection. Additionally, the Charter of Fundamental Rights of European Union (2010) provides further protection of personal data. Article 8 of the Charter protects individuals against the intervention of a state. The key legal document protecting personal data is General Data Protection Regulation (GDPR) which governs how companies could process personal data. Under the GDPR, the processing involves any activation which could be pursued with personal data (Article 4(2) GDPR). The 'personal data' is defined as any information, acquired by a company, which relates to natural persons, and allows for their potential identification (including their location, or IP) (Article 4(1) GDPR). The GDPR also introduced clarity of its regime by defining key issues, such as the definition of 'data subject' which encompasses any person of whom data is collected (Article 4(1)), and 'data controller' which refers to any person (either natural or legal) that process the acquired data (Article 4(7)). Importantly, the key feature of the GDPR's regime is a user's 'consent', which must be unambiguous, specific, informed and freely given. The GDPR represents a twofold nature: individuals are asked to consent for any data processing making it clear that a digital platform or services would rely on their data and consequently have a right to be informed about the way their data would be processed, whereas the data controlled is obliged to perform the data processing obligations with the guarantee that the data would be processed to the extent which is well-grounded and demonstrable as agreed by individuals. Hence, the GDPR strengthened the protection of personal data and, simultaneously the privacy of users.

Facebook Case: Is There A Way To Acknowledge Data Protection And Competition Law Together?

EU law appears to not recognise the intersection between that data protection and competition law. Primarily in Asnef-Equifax (2006), the Court of Justice of European Union (CJEU) rejected the interplay between competition law and data protection rules by stressing that data protection law is outside the scope of competition legal order. Presently, with the evolvement of the Digital Markets Act and Digital Services Act, future enforcement will draw an attention to actions of online intermediaries. Potentially, this could abandon the isolation of data protection principles from an anticompetitive assessment. The EU legal practice contributed to the identification of different phases of the development of the intersection between competition law and data protection. Concurrently, however, there remains no consensus as to the optimal method of evaluating data in the EU competition law cases and the impact of the data protection concern on the goals of competition law. It is apparent that EU competition law is based on an orthodox approach and assesses decisions involving data through the spectrum of keeping a competitive equilibrium in hypothetical markets.

This section discusses the Facebook case from German Competition Authority (BKA). The case could be seen as the prime example of recognising a relationship between competition law and privacy at the Member State level. It could serve as a first attempt to define privacy from a competition law perspective, noting potential connection between these two areas of law.

Facts of the Case

The BKA began its investigation against Facebook due to apparent abuse of dominance in the social media market. During the investigation, the BKA closely analysed Facebook's Ts&Cs and concluded that some provisions were unfair to its users. Facebook's position

allowed the platform to acquire and analyse the data of Facebook, WhatsApp, Instagram, Oculus and Masquerade users as well as the data coming from any websites/apps that use 'Facebook Business Tools'. This case could serve as an interesting example of the competition authorities trying to provide elements of certainty to the debate on the data protection influence on competition law.

Interestingly, competition on the social network market remains low. For digital services, advertising-financed profits are key elements to innovate. Hence, the personal data of private users remains a key aspect of their revenues. Facebook's position on the market was exceptionally high, as concluded by the BKA, which based its conclusions on the elements such as indirect network effect or access to data.

Unquestionably, there has been a behavioural element of users identified, which made it difficult for users to suddenly change the platform into another: users were more likely to stay locked into a platform due to the presence of their peers or family on the platform. In addition, Facebook demonstrated a strong network effect, since the platform was capable of offering targeted advertising, based on Facebook's business model. In response, Facebook was in a position to gather a large quantity of users' data, and subsequently could link personal profiles between Facebook-owned platforms and third-parties using Facebook Business Tools. In this respect, Facebook was capable of acquiring data from the so-called travelling website; this initiated a possibility of personalised pricing.

Legal Perspective

While assessing the exploitative theories of harm, the BKA found that Facebook's Ts&Cs allowed for a wide data acquisition from a variety of sources, which included the Facebook platform's data, and any device-related data from sources outside Facebook. Subsequently, the gathered data was merged together (Facebook case: press release 2019).

Unquestionably, an act of exploitative business terms amounted to Facebook's abuse of dominant position. Under the EU competition legal order, exploitative abuses are prohibited under Article 102 TFEU, and the caselaw interpreted them as including prohibition of predatory pricing, unfair pricing, or unfair trading conditions (United Brands 1978, para 248; Ministère public v Jean-Louis Tournier 1989, para 34). Hence, it remains accepted that unfair trading terms or price could be inequitable as to its effect on competitors. In addition, as per United Brands (1978) case, discriminatory trading terms or provision could also form abuse of dominance due to its negative effect on consumers (p. 248).

The BKA was very cautious in the GDPR consideration while assessing the competition law infringement. Generally, the EU competition law disregards any application of the privacy-related concerns to the competition law assessment, since it is beyond the scope of EU competition law to consider the data related infringements. However, the BKA, in its assessment, relied on the German Federal Court of Justice approach. Such approach directed that competition rules might be used to justify the protection of constitutional rights since a dominant market position prescribed an unlawful privilege to terminate the autonomy of contracts (Facebook case: press release 2019, p.7). In fact, the infringement of the GDPR might not amount to competitive harm in itself. In the assessment, the BKA took an accumulative approach, which indicated that the GDPR infringement was relevant from the perspective of competition law; Facebook's market position's abuse was capable of incorporating elements of the GDPR infringement.

The Aftermath **o**f **t**he Case

The BKA's proceeding was not the end of the saga. Later, the Higher Regional Court of Düsseldorf stopped the execution of the BKA's decision in interim proceedings, stating that – among several other weaknesses – the decision lacked a convincing theory of harm.

In 2020, the German Federal Court of Justice (BGH) issued a decision that confirmed the enforceability of the BKA's order against Facebook's data practice. The case focused on the interplay between competition law and collection of data. The BGH turns down any idea of "attention markets" and instead defines what Facebook actually offers to users. Yet, there is a uniqueness of Facebook market, it cannot be contrasted with platforms such as LinkedIn or Twitter. The BGH clarified that the question should not be solely based on the data protection reasoning, as to whether Facebook violated the GDPR. In fact, the emphasis should be placed on the competition distortion caused by Facebook's terms on the ground that the users are offered no choice how their data is combined for purposes of personalisation. In this respect, the BGH established that (i) Facebook's users could wish to use the Facebook social network services with more intense personalisation of their experience, or (ii) the users consented only to personalisation based on the data that they reveal on Facebook itself.

The case is now being referred to the CJEU, asking, inter alia, whether competition law could be infringed by violating GDPR. It appears that the division and connection upon this subject could be emblematic in many respects. Having analysed the legal background, the analysis of the cases provided further ambiguities in the debate on intersection between competition law and privacy. The next section focuses on assessment of privacy within competition law. The debate will acknowledge its societal and legal importance, drawing notice to any apparent connections and divisions.

How To Define Privacy In Competition Law Sphere: Between The Legal And Social Importance

The importance of data in society could be seen as a non-economic activity since it aims at benefiting all members of society. Potentially, the concept of social welfare could be important at capturing problems that could lead to a market that create goods which are not

considered as important for the general welfare. Yet, social welfare is perceived as being a separate stream in case law, to which different criteria apply (Albany, 1999, para 84). Arguably, privacy is a complex matter from the competition law perspective.

From a practical view, the true value of data remains unknown. Importantly, data does not translate into money immediately. Kennedy (2017) argued that essentially data-rich companies are a significant source of innovation. Although consumer welfare promotion is a recognised goal of EU competition law, it can be deduced that the 'ultimate' goal of competition law is to ensure the effectiveness of competition in the internal market, which aims at increasing consumers welfare (Österreichische Postsparkasse and Bankfür Arbeitund Wirtschaft, 2006, para 115). Yet, these goals are interchangeably affecting each other, as distorted competitive processes may directly or indirectly harm consumers.

Furthermore, conflicts between competition law and social concerns originate from the markets where a Member State introduced competition. Companies create profiles about their consumers and collect data on them; such logic has been already applied in the health privacy context. Hence, the market gained power as a prerogative of the state, by governing society and gathering data, and where a market took a responsibly for any public interest, recognising the acknowledgement of non-economic objectives (Gerbrandy, 2019). Accumulation of consumers' data may enable behavioural targeting by advertising. Yet, it remains unclear how to encompass data protection principles into competition law assessments. Initially, the assessment should be based on restoring effective competitive process, which is the heart of the EU internal market, and consider all other protections only to ensure that there were no gaps in a type of protection. The test involved could be based on balancing the competition law and the protection of public concerns or imposing a privacy monitoring infrastructure necessary for competition law authorities.

In fact, privacy protection does not have a recognisable definition. The definition is broad and encompasses an importance of personal privacy, to their political affiliation, social life or dignity, which might be a goal on its own. In many respects, the protection of privacy is considered to be beyond the scope of competition policy. It has been already widely noted that privacy invasions and data breaches are increasingly presenting a danger to society. In theory, some of the competition enforcements might be capable of considering the increased consequences of commercial processing or collection of personal data. Yet, neither competition law nor economic analysis support such an argument (Kimmerlman, Cooper 2017). There are varying perspectives of privacy recognised globally as to the level of data protection and the role of competition law in this context. Different conceptions of privacy might be recognised in various cultures and social systems or the consumers' heterogeneity: some might value privacy less, whereas others much more.

The concept of privacy might be defined both in a broad and narrow sense. Unquestionably, any breaches of privacy affect a great number of peoples and could potentially compromise the process of democracy (Tsai, Egelman, Cranor, 2011). Yet, the precise contours of privacy effect constitute a subject of extensive academic discussion. Many perceived the EU legal order as offering the most attractive personal data protection. The protection of data protection is encompassed both in the TFEU and the Chapter of Fundamental Rights of European Union. In fact, the most emphasis should be placed on the GDPR, which serves as the key document for data protection. The GDPR's fundamental principle is the requirement to establish a legal basis for personal data processing, requiring of a data subject's explicit consent. Under the GDPR, the processing involves any activation which could be pursued with personal data, defined as any information acquired relating to natural persons, and allows for their potential identification. The GDPR strengthened the protection of personal data and, simultaneously,users' privacy.

The GDPR sets a basic requirement for the effectiveness of the legal consent for the data processing, which requires the consent to be specific, unambiguous, freely given and informed; granted by individuals by clear affirmative action, or by a statement, which signifies a consent to proceed their personal data. In this respect, the GDPR represents a twofold nature. Firstly, individuals are asked to consent for any data proceeding making it clear that a digital platform or services would rely on their data and consequently have a right to be informed about the way their data would be proceeded. Secondly, the data controller is obliged to perform the data processing obligations with the guarantee that the data would be processed to the extent which is well-grounded and demonstrable, as agreed by individuals.

As per the Breyer (2016) case, the concept of personal data appears to have a broad scope of applicability, with many arguing that personal data protection became 'law of everything.' (Purtova, 2017) Arguably, any use of personal data, even, for instance, by algorithms, falls within the scope of the GDPR, since Article 4(2) GDPR broadly defined processing of personal data as:

> "… any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration or otherwise making available, alignment or combination, restriction, erasure or destruction."

Generally, there is no ex-ante choice available to the individuals, under the EU data protection law, as to whether they want their personal data to be processed. Although consent is required, individuals are unable to thoroughly consent to a real purpose of data processions.

An attempt to define privacy from a competition law perspective could be witnessed by the BKA's Facebook case. The assessment of the privacy protection rights in the case begins with a simple principle: personal data processing can only take place once data subjects agreed to their data being processed, or when data processing is granted by the law. The BKA took an

approach of a data protection authority and explained that the Facebook's Ts&Cs were deemed as appropriate within the remits of the GDPR. The BKA noted several points from privacy protection's perspective. According to the case, the Facebook users were not aware of the means to which Facebook collected and processed their personal data. It amounted to an ungenuine and poorly-grounded consent from their users. Hence, users were not likely to expect that Facebook also analysed the data from different websites (Facebook case 2019, para 778-780).

Furthermore, the BKA concluded that the Facebook's Ts&Cs were complex, written in arduous to understand language; it was difficult to fully comprehend the real intention of the platform, especially in the purposes of data processing, Consequently, the users' consent was not seen as specific, informed, or freely given within the GDPR remits, as Facebook required data from a number of sources; the platform later combined the data acquired from Facebook and third-party sources. The BKA concluded that the conduct of data combination was unlawful as:

> "[p]rocessing data from third-party sources to the extent determined by Facebook in its terms and conditions is neither required for offering the social network as such nor for monetising the network through personalised advertising, as a personalised network could also be based to a large extent on the user data processed in the context of operating the social network." (Facebook case, 2019, para 10).

However, the BKA insisted that the consent of users might be seen as being forced since in the opinion of the BKA: "[v]oluntary consent to [users'] information being processed cannot be assumed if their consent is a prerequisite for using the Facebook.com service in the first place." (Facebook case, 2019, para 10) The BKA added that combining data from various sources was seen as a feature not necessary for the functioning of the social network. Hence, such conduct was not conditioned to users' consent and constituted a privacy breach.

Yet, within the scope of the BKA's judgement, nothing indicated that the GDPR's consent requirement was grounded on the market power of the data controller. The GDPR remains silent on the theory of competitive harm and does not distinguish on the market power basis and remains silent as to the dominant firms' responsibility to resemble special privacy responsibility. Hence, the definition of privacy violations is difficult to be ascertained by anticompetitive means. Returning to the BKA's proceeding, the Facebook's conduct amounted to privacy harm, since the precise purpose for data acquisition and processing purposes remained undefined and unclear for consumers. The BKA concluded that the privacy harms could amount to a cognisable competition law injury, indicating that the reason behind their rationale was to target Facebook's strategy to accumulate data. Besides, the conduct in question was seen as violating the right to informational self-determination, which aims to secure individuals' right to decide freely on the processing of the personal data, which the BKA stressed to be linked with the dominant market position. Furthermore, the BKA, in their assessment, relied on the German case law, which established that the market power could be further evidenced by abusive terms of business. In this respect, the case appropriateness of unbalanced negotiations was capable of being applied into different areas of law, as well as data protection law, which also aims at ensuring a right to informational self-determination. The BKA applied the German competition law to resolve the issue and used the data protection law as a benchmark to establish the abusive nature of Facebook's conditions.

In this respect, the intersection between competition law and privacy protection is complicated and goes beyond the boundaries of competition law enforcement. The concept of privacy is a social practice and remains difficult to be defined. The users can rarely contract with the platform providers on the level of privacy, as only a mere assurance would be put forward to the end of the matter. The digital society is constantly evolving and introducing new

threats and vulnerabilities, which made the relationship between data protection and competition law even more complex as beset by asymmetric information.

Further Implications

The aspects relating to the privacy protectionism remains not exclusively defined by the BKA's case. In addition, at the European level, the matters between competition law and privacy protections were noted to be not mutually interlinked in the case of Asnef-Equifax (2016), where the CJEU indicated that: "any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection." Simultaneously, the vertical merger of TeleAtlas/TomTom (2008) did not raise any data issues and kept a prudent approach in excluding data protection arguments in its assessment. Nevertheless, the EU Commission defined a narrow market product of digital maps, potentially acknowledging the digital data in market definition. However, in Microsoft/LinkedIn (2017), the Commission offered a more mature approach to data within EU competition law, as the Commission relied on that the users 'privacy protection to assume the impact of combining the two companies 'databases. Interestingly, the decision referred to the GDPR, which at the time of the assessment had not been applicable and announced that the GDPR would empower individuals with control over their data and limit Microsoft's ability to access and process personal data of the users. Nevertheless, the Commission did not preclude Microsoft's access to LinkedIn's data after the merger. Yet, the Commission defined two horizontal issues following the merger. Firstly, there was no distortion to competition as pre-merger the companies were competitors on the hypothetical market. Secondly, Microsoft and LinkedIn, after a merger, would combine their databases and achieve market power, resulting in higher barriers to entry. The Commission

focused on securing a competitive process and did not provide any guidance on data protection within competition law sphere.

Hence, no consensus remains as to an optimal method of evaluating data in EU competition law. According to Phelps, the economic value of privacy might be twofold (Phelps, Nowag, 2000). In fact, privacy might bear positive connotation, and serve as an intermediate good, in situations where nondisclosure of data is beneficial for a data subject, or when users decide to disclose their personal data in order to obtain a monetary payment (Kerber, 2016). Hence, it is likely to conclude that privacy to some extent might assign a certain monetary value. On the contrary, privacy might also serve as a final good. Botta (2019) argued that such a dimension represents only a normative dimension, and noted that its legal character was stated in Article 8 of the Charter of Fundamental Rights. Yet, the privacy in itself is a very complex and diverse concept, and the nature of its sensitivity might be different through different societies.

It is apparent that EU competition law supports the prevailing approach and assesses decisions involving personal data through the spectrum of protecting a competitive equilibrium in hypothetical markets. As it has been emptied before, the concept of privacy appears to be a multi-dimensional and dynamic issue. Thus, it is requiring careful considerations of all dimensions and interests of parties on relevant markets (Thibodeau, 2014). Both data protection and competition legal orders seek the advancement of market integration and share a concern for the welfare of individuals, with consumers benefiting from the collection of their data in a wide array of free services, products or contents. Thus, data protection and competition law could possibly intersect with each other and keep balanced during an assessment of anticompetitive misconducts. Yet, although data protection principles begin to influence competition authorities, the protection of the individuals' rights as consumers and market participants is already protected by the data protection and consumer protection authorities.

Conclusions

Both data protection and competition legal order seek the advancement of market integration, and both share a concern for the welfare of individuals, with consumers benefiting from the collection of their data in a wide array of free services, product or contents. The acquisition of big data does not immediately result in anticompetitive conducts. However, a handful of technology undertakings exercise control over a large quantity of personal data and its processing, with a focus on personal practices. Data collection on an unprecedented scale put the privacy of the end-users into danger. As a result, the changing economic landscape brings uncertainty to the nature of the competition pressures, with an emphasis being given on the normative scope of competition enforcement — mainly as to whether the EU competition law could be viewed as a societal norm also advancing the wealth.

One might encounter a paradoxical relationship, as the EU competition law aims at both achieving a well-functioning, competitive market as well as preventing consumer harm. This is, thus, unclear to determine what the potential stance for competition law could be. It is difficult to engage in an analysis of the long-term interest of consumer for dynamic efficiencies. Furthermore, privacy and data protection are recognised in the European Charter of Fundamental Rights as fundamental human rights, and data protection law — GDPR. According to the EU data protection, the growing economic significance of data requires adoption of a new concept of consumer harm, which adopts an evolutionary interpretation of the current competition enforcement, especially the abuse of market dominance concept. In this respect, it still remains unresolved whether privacy could serve as an element of competition law realm.

BKA. (2019). *Case B6-22/16 Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing. Press Release*. Retrieved August 28, 2019 <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108>

Botta, M. and Wiedemann, K., 2019. The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey. *SSRN Electronic Journal*,.

Case 27/76 United Brands Company and United Brands Continentaal BV v. Commission, [1978], ECR 207

Case 395/87 Ministère public v. Jean-Louis Tournier, [1989] ECR 2521

Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios ECR I-11125. [2006].

Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland judgment of 19 October 2016

Case M.8124 Microsoft/LinkedIn, 14 October 2016

EDPS. (2016). *On the coherent enforcement of fundamental rights in the age of big data* (Opinion 8/2016). Retrieved July 22, 2019 https://www.huntonprivacyblog.com/wp-content/uploads/ sites/28/2016/10/14-03-26_competitition_law_big_data_EN.pdf

EU General Data Protection Regulation (GDPR). *Regulation*, *2016*(679).

European Commission, (2004). Commission Notice Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty, 2004/C 101/07.

European Commission (2009). Guidelines on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, (OJ C45/02)

European Commission, (2011). Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements. OJ C 11/1

Hubert, P., & Combet, L. (2011). Exploitative abuse: The end of the Paradox? *Doctrines l Concurrences, 1*, 44-51.

Joined Cases T-213/01 and T-214/01 Österreichische Postsparkasse and Bankfür Arbeitund Wirtschaft v Commission [2006] ECRII-1601

Kerber, W., 2016. [online] Econstor.eu. Available at: <https://www.econstor.eu/bitstream/10419/144679/1/850599016.pdf> [Accessed 5 April 2021].

Kimmelman, G. and Cooper, M., 2021. *A communications oligopoly on steroids - Equitable Growth*. [online] Equitable Growth. Available at: <https://equitablegrowth.org/research-paper/communications-oligopoly-steroids/> [Accessed 5 April 2021].

Phelps, J., Nowak, G, 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1)

Purtova, N., 2017. The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law. *SSRN Electronic Journal*,.

Satariano, A., 2021. *Facebook Loses Antitrust Decision in Germany Over Data Collection*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html> [Accessed 5 April 2021].

Thibodeau, P. (2014). *The Internet of Things Could Encroach on Personal Privacy*. Retrieved October 2, 2019 https://www.computerworld.com/article/2488949/emerging-technology/the-internet-of-things- could-encroach-on-personal-privacy.htm

TomTom/Tele Atlas, Case No COMP/M.4854, Decision of 14.5.2008

Tsai, J., Egelman, S., Cranor, L. and Acquisti, A., 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 22(2), pp.254-268.