Competition Commission of India
Journal on Competition Law and Policy

Doi: 10.54425/ccijoclp.v3.42
Vol. 3, December 2022, pp. 79-95

Data Privacy at the Altar of Competition Laws

Rupal Nayal[1]

Abstract

Data privacy has been receiving widespread attention. However, in some areas, dedicated laws are proving inadequate to deal with the impact of anti-competitive effects on the privacy of users. This requires a detailed discussion on the unilateral privacy policies imposed by data giants involving consent notices in the nature of "take it or leave it". It further brings into question the role that competition law can play in examining abuse of dominance within firms, where users are being held captive and forced to share access to their data, given the status of the players in the market.

Keywords: competition, privacy, antitrust, GDPR, WhatsApp, Facebook, lock-in, Bundeskartellamt, antitrust

1. Introduction

The digital economy rests on the pillars of interoperability and information exchange—so much so that the 2010s ended with the proclamation that "data is the new oil" (Arthur, 2021). The growing importance of consumer data is accompanied by questions of adequate security. The Supreme Court, in *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.* (2017), observed that consumer data is threatened by state as well as non-state entities.

Data has become a valuable entity and its generation can go a long way in making digital systems efficient. Almost every aspect of life involves the transaction of data. The internet has been the cradle for digital platforms, which have manifested in online infrastructure, wherein they work to facilitate user interactions and transactions, such as collecting, sorting, or interpreting personal data either remotely or as a crucial part of their

[1]LLM, National Law University Delhi; rupal.nayal21@nludelhi.ac.in

business structure (Moshell, 2005). Data has also become a revolutionary tool in changing the manner in which businesses and their decision-making processes are conducted. Businesses are now incentivised to create data banks that can record consumer preferences, which can later be used to target consumer behaviour through advertising (Nissenbaum, 2010).

People across the world have become increasingly reliant on the internet to conduct everyday businesses, signalling a digital revolution, which was further reinforced by the new environment created by the COVID-19 pandemic, which resulted in people being confined to their homes. While this resulted in great potential to provide better services to users, it also led to an explosion of data, which makes it imperative to be cautious about how our data is used and our consent derived for doing so.

The collection of users' personal data has been a part of the business model of online platforms since the beginning and was not something that faced much objection. However, with greater convergence of consumer needs and digital intermediaries, such companies gained greater access to personal information, which was unprecedented.

2. Significance of Data Privacy

As a natural corollary, this takes us to the larger concern of data privacy, to which big data companies pose a substantial threat. In recent years, there has been a significant recognition in the right to privacy. In the context of digital platforms, it can be defined as the entitlement of an individual to control a piece of information about them exchanged through the online mode.

Digital platforms are not only acquiring data directly by taking permission from users but also tracking their online activities, choices, and preferences in order to benefit from targeted advertising, for which users do not give informed consent in most cases, especially in emerging economies, given the lack of awareness. This can have a significant influence on user behaviour and decision-making processes. Thus, it has often led to the proposition that these services can no longer be called "free", since users pay for them with their personal information. The privacy of users is not only threatened by the possible abuse of their data for profit maximisation but also the lack of safeguards to prevent the data

from falling into dangerous hands. Some software, such as Amazon's Alexa or Apple's Siri, are even known to pervade the boundaries of one's personal life by listening to users at all times.

There are various domains within which privacy is threatened. First is personal information which, after being pooled with external data, could translate into newer information for which consent may not have been granted. Personal data refers to data or material that can lead to the identification of a person. Second is sensitive data, which might be kept and managed at a site with inadequate security, making concerns around data leak more pronounced (Mehmood, 2016).

Even though a majority of online sites claim to take the consent of users about their data being used, often, consumers are not aware of the purpose and consequences of how their data might end up being utilised. There is a chance that a person finds it difficult to retain control over their data in the event that a digital repository containing their data is created (Hogben, 2007). It has been observed that most digital platforms harbour a bias against the data privacy of consumers, as demonstrated by the provision of inadequate privacy controls or practices of storing data as well as instances of abuse by the third party, as exemplified in the Cambridge Analytica scandal. The controversy highlighted the power of digital platforms and political consequences of threats to privacy (Wasastjerna, 2019).

Additional to this are the ways in which digital platforms feel entitled to alter their privacy policies in an arbitrary manner. This often reeks of an attempt to gather large volumes of user data along with an irreversible right to own and utilise it. The act of accumulating such data hampers the privacy of users, more so when digital platforms are not ready to acknowledge it, instead belittling it as something inconsequential (Mal & Parikh, 2011).

Various jurisdictions have contemplated data protection legislations in order to address these concerns. The objective of these laws is to provide data subjects with a certain degree of control over data that belongs to them or is generated through their online activities, while enabling them to set boundaries with regard to its accumulation and utilisation. The most prominent measure in this regard came from the European Union in the form of the General Data Protection Regulation (GDPR). GDPR delineates

the rights to be conferred on data subjects as well as the obligations to be acted upon by data controllers. The latter is required to establish reasonable grounds before they resort to processing data, which needs to be exercised by consent from the data subject.

In India, the Personal Data Protection Bill was introduced with a similar intent; however, it is yet to be enacted. Section 11 of the proposed law deals with the consent of data principal. It provides that, in order to process personal data, it is imperative to obtain consent from the principal, which should not only be free, informed, specific, clear, and capable of being withdrawn, but "The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose."

3. WhatsApp Privacy Policy 2021

On 4 January 2021, users of WhatsApp LLC woke up to a notification on their phones which asked them to accept data from their interactions with business accounts being shared with Facebook to expand the latter's marketing and advertising; if users declined, they would be unable to use WhatsApp's services after 8 February 2021, which was subsequently postponed to 15 May 2021.

A notable point in this policy was that the data sharing arrangement did not apply to users residing in the European region due to negotiations with data protection regulators in Europe ("WhatsApp and Facebook to Share Users' Data Outside Europe and UK," 2021). Thus, it can be inferred that Indian users were subjected to these terms in the absence of robust data protection legislation. However, following the outrage over this development, the Competition Commission of India stepped up and initiated a suo moto investigation (CCI Suo Moto Case No. 01 of 2021) into the matter under Section 26(1) of the Competition Act.

It was observed that, previously, in a case brought against the privacy policy of WhatsApp in 2016, the latter had provided an alternative to users where they could "opt out" of the data sharing arrangement with Facebook (*V. K. Gupta v. WhatsApp Inc.*, 2016). However, Facebook, which is the purported major beneficiary of this new privacy policy if things go through, refused to be arraigned as a party to these proceedings.

The Commission made it clear that this issue is not in the sole purview of data protection law, since large-scale collection of data and its consequent use can serve to provide competitive leverage to dominant firms, which may then resort to exploitative and exclusionary tactics, thus making it a subject to be scrutinised by competition authorities as well. The Commission was of the view that this case fell under abuse of dominance by a dominant player in the relevant market under Section 4 of the Act, and they were authorised by Section 33 to prevent such practices. The issue of WhatsApp being a dominant firm within a relevant market was settled in the case brought by Harshita Chawla (CCI Case No. 15, 2020). It was observed that this position was still prevalent. Thus, the Commission arrived at the conclusion that prima facie opinion could be formed that this issue should be subject to a detailed investigation in view of the "take it or leave it" policy. Subsequent to this, a petition was filed in the Delhi High Court which challenged this order on the ground that the matter related to similar issues was sub-judice (*WhatsApp LLC v. CCI & Anr.*, 2021). The Court dismissed the petition, acknowledging the jurisdiction of the Commission in probing the matter; however, questions regarding the validity of such orders and their feasibility remain open. This leads us to ponder over the prevailing discourse, taking into account antitrust considerations in concerns over data privacy.

4. Probing Interactions with Competition Law

The anxieties surrounding data privacy are further heightened with mergers of data giants. These mergers result in increasing the joint repository of data, which would give the entity constituted after the merger even greater power and tools to process personal data, thus hampering privacy, especially in cases where consent was taken for data utilisation by only one of the pre-merger companies (Stucke & Grunes, 2016). Such sharing of data is often effectuated through privacy policies worded in the form of standard contracts or business transfer clauses. The take-it-or-leave-it nature of these policies tends to force users into accepting conditions that subject the privacy of their personal data to unwarranted intrusion.

The inherent intent of competition law is to enhance the welfare of consumers and curb business practices that might have a negative effect

on the well-being of consumers. In addition to this, its objectives include establishing an environment where competition can flourish based on a level playing field in a manner that not only safeguards economic efficiency but also promotes consumer choice embedded in fairness (Balto & Lane, 2019).

One of the earliest instances that witnessed the intersection of competition law with the domain of data privacy was the acquisition of DoubleClick by Google. This merger came under the radar of the Federal Trade Commission (FTC), since both companies possessed large volumes of data related to the online search and browsing behaviour of users and such substantial amalgamation of data was a cause for concern ("Statement of FTC," 2007). However, this merger came on the radar of the FTC and the European Commission since these companies were not considered potential competitors. The European Commission also stated that its decision was based merely on competitive considerations and was isolated by the data-related obligations of the companies. Thus, it can be inferred that the decision was based on a narrow interpretation employed by FTC and was restricted to the quality and amount of personal data that would exist in the market after the merger takes effect. It failed to take into consideration the interests of all relevant parties, as stated in the dissenting note by Pamela Jones Harbour, since the antitrust analysis failed to consider the values of user data that are to be ultimately collected and utilised (Lee, 2020).

Another encounter was observed during Facebook's acquisition of WhatsApp. Although the merger was given authorisation, the FTC director made it clear that this does not mean that the assurances provided in WhatsApp's privacy policy would be invalidated nor that it would affect the statements given in regard to privacy by both companies. It was stated that there should not be any considerable alterations to the way in which data already collected from WhatsApp users is used in the absence of explicit consent or any falsifications about how that data is stored (Kimmel & Kestenbaum, 2014). However, as mentioned above, in 2016, the privacy policy was updated, wherein it was stated that, in order to improve customer experience, WhatsApp data would be shared with Facebook (WhatsApp, 2016). Consequently, the European Union fined Facebook EUR 110 million, penalising the company for providing

misleading information regarding the possibility of automated matching of users' accounts across both apps (European Commission, 2017).

The Organisation for Economic Development (OECD) has been wary of the potential harm these mergers could cause, since dominant firms could impose the unfair terms of their privacy policies for the accumulation of data across different business entities by virtue of their market position (OECD, 2020). This might lead to "cross-service" data sharing, giving firms the opportunity to take advantage of their dominance in the adjacent market

Taking this into account, FTC is of the view that it needs to be ascertained whether or not combining the data sets of both companies would lead to power concentration in the market. There is also a possibility that, after the merger, the new entity might enforce privacy policies which might be harmful for data protection, especially in situations where users are asked to give away more than necessary data without being given a choice to accept or reject those. Such possibilities need to be considered while reviewing a merger. This was seen during the merger review process, when Facebook denied any possibility of such synchronisation but attempted to do so post the merger (Niu, 2016).

Advocates of maintaining separate domains for data privacy and competition premise their argument on the underpinnings of competition law essentially on price competition. They opine that, in the absence of price, a market cannot be constituted, and hence, there would be no market power. However, a narrow approach to competition makes consumers vulnerable to harm that can be caused by non-price factors such as privacy (Mehmood, 2016).

Choice and privacy cannot be seen as mutually exclusive, which entails that the regulation of both cannot be bound in watertight compartments. When big data companies seek data to be collected, stored, and processed, concerns around competition and privacy are bound to follow. A unilateral modification in privacy policy points to a situation where users are locked in, with limited to absolutely no bargaining power to express their disagreement with the new update. Even though data privacy ought to be the primary governing space of data protection authorities, it has been suggested that, in circumstances where the subject matter seems to overlap the need for both regulations, authorities should not shy

away from exercising their powers and rendering them open to scrutiny (Stojanovic, 2020).

Some scholars (Ezrachi & Robertson, 2019) have proposed that competition law should be taken as a supplementary stratum in shielding cases where data collection by dominant firms is involved. They attempt to analogise excessive prices with excessive data collection. If this is followed, antitrust regulators would be able to ascertain whether the criteria for adequate prices is justified; if not, it would constitute unfair business practices, thereby putting competition in the market at risk.

5. Privacy-Competition Präzedenzfall (German for "precedent")

After Facebook acquired WhatsApp in 2014, the Bundeskartellamt, the antitrust regulator of Germany, initiated an investigation against Facebook over suspicions that there were violations of data protection regulations riding on its dominance in the market, more specifically abuse of dominance (Bundeskartellamt, 2016). It was observed that the terms of the policy effectively meant that users could use the services only if the terms were agreed to, which postulated that Facebook would be gathering data external to the website, expanding to its subsidiaries and even third-party sites that embedded Facebook buttons.

The authority gave its ruling in 2019, according to which the act of imposing such terms amounted to an abuse of dominant position in the market, since those terms violated the principles of GDPR. Thus, it was found that competition law was infringed upon when there is transgression of data protection regulation and its constituent. As far as consent is concerned, it was ruled that the users did not really have "free choice", since there is a strong imbalance between the position of the company and the users (Bundeskartellamt, 2019).

The decision was based on the theory that it was the dominance of Facebook in the market of social network that made it powerful enough to impose one-sided terms on users to give permission to be tracked by Facebook; therefore, consent was reduced to a mere formality (Mehmood, 2016). The investigation was rooted in the proposition that data protection law could be located as the criterion for determining whether certain terms were unfair and anti-competitive as per the Treaty on the Functioning of European Union's Article 102 (Graef *et al.*, 2018). Andreas Mundt,

President of Bundeskartellamt, while announcing the decision, made an important comment in this regard, stating that asking for a mandatory agreement to the terms and conditions was not a sufficient basis on which a large volume of data processing could be operated. In this event, the consent given could not be considered free (Bundeskartellamt, 2019).

However, the Regional High Court of Düsseldorf (Oberlandesgericht Düsseldorf/OLG Düsseldorf) refused to uphold the decision until the decision of the court in the main proceedings since they were not clear on the validity of the impugned order. The court was not convinced that violation of data protection could be held as a benchmark to decide whether a firm's conduct was the result of abuse of its dominance and thus, formed an impediment to the objectives of competition law. From the perspective of antitrust, the authority was not convinced that the decision of the user to provide consent for data sharing is based on network effects following from the dominant position of Facebook (Düsseldorf, 2019).

The observers found this decision by OLG to be extreme since their reasoning was found to be isolated from the potential of such firms to gather data to fortify their power in the market and raise barriers for new entrants, thereby being detrimental to competition. This was in confirmation of the European court's opinion that the connection between abuse and dominance does not demand to be the only link per se, and it would suffice if the conduct emboldens the firm's position (Van den Bergh & Weber, 2021).

It is also imperative to highlight that price is only one of the many dimensions surrounding antitrust concerns, innovation, choice, and quality being the other critical factors. When it comes to the operation of perfect competition in digital markets, where services are essentially offered for "free", the significance of the latter aspects becomes even more profound, especially regarding possible reduction in data privacy. Concealed data practices (Kemp, 2020) imposed by dominant players also create an exclusionary effect for other players in the market by creating higher entry barriers (Valetti, 2019). This is exercised by the data giant leveraging the accumulated data, often spilling the impact over to tied markets, in effect foreclosing the market for rivals.

In a change of circumstances, on 23 June 2020, the German Federal Court of Justice reversed the OLG decision and ruled in favour of the

antitrust authority (*Bundeskartellamt v. Facebook Inc.*, 2019). It is believed that this decision will go a long way towards strengthening the resolve of competition regulators in helping governments put a leash on the leviathan data-gathering activities of big data giants. The Court found the unfair terms to be abusive, especially since Facebook refused to give users a real choice. Judge Peter Meier Beck was of the view that users should be served with an adequate choice, and under no circumstance should Facebook's dominant power prevail over the free choice and decision-making autonomy of users.

6. Delving Into Lock-In and Network Effect

Lock-in effect refers to a situation in which consumers find it difficult to switch from one service to another due to substantial costs. In the framework of data, since consumers have been using the services of digital platforms for a considerable period, a substantial amount of correspondence and network has been built on the service. The network of the data subject may consist of hundreds of people, ranging from family to friends to colleagues, all of whom cannot be expected to switch to another, safer privacy haven.

There is an implicit compulsion upon the user to continue using the service to stay connected to members of importance who will not be available on other services. The prevalence of WhatsApp class and office groups, where important instructions are routinely shared, cannot be denied. Thus, not agreeing to the terms imposed by the platform would land the subject in a situation where they risk losing not only access to personal information but also connections built over the years, affecting personal, social, and professional networks. This, in turn, gives rise to network effects, where additional users add to the existing pool of users. This happens because the platforms seem more attractive to a new user, since almost all the people from different spheres of their lives are already a part of it (Buiten, 2019).

Even we if consider that the user may be part of other forms of social media communication, the all-encompassing status of certain digital behemoths such as Facebook, which exercise control over other services such as Instagram or applications that require a Facebook account, adds to the concern. In this context, the consent given to a set of terms and

conditions imposed by a service cannot be considered meaningful, since a genuine choice needs to be laced with the alternative of declining without fear of consequences (Complaint under Article 77(1) GDPR, 2020).

Consumers constitute a crucial class that benefits from competition in terms of commensurate pricing, adequate quality, and a range of alternatives to choose from. When confronted with a policy that does not give them the opportunity to negotiate, they are deprived of their part in a contract. The role of competition law does not expect it to be concerned with the processing of personal data and its subsequent use. Rather, competition law aims to investigate whether users are unable to exercise a real choice in accepting certain terms and conditions due to the dominant position of the platform in the market. After the criterion of dominance has been fulfilled, the next step is identifying the abuse it leads to, which might be in the form of invading the privacy of users by collecting data for purposes that they might not have agreed to otherwise (Wahyuningtyas, 2017).

This is a competition issue in more ways than meets the eye, since the inability of users to move to another service reinforces the already strong position of the platform. This not only acts as an impediment to the entry of new platforms, but the large amount of data concentrated by these platforms puts privacy at risk, giving increased leverage to the data giant (Bundeskartellamt, 2019).

The case of WhatsApp exemplifies the impact of these effects, along with the implications of consent, thus establishing its dominant position in the market. On the back of its dominant position, it seeks to milk the agreement of users over unfair terms, which has a direct correlation with its formidable network effect. It has also been observed that the way in which users' data is monetised by Facebook after cross-sharing amounts to abusive conduct (IFF, 2021).

7. Exploring Possibilities

The proposition of competition law not encroaching on the domains of privacy could have been considered if the impact of market failures and policies were not interdependent. Assuming that issues of competition, which include cartels, mergers, and dominant platforms, are isolated from concerns of informational privacy and data would be myopic. Even

if data protection laws lay down a maximum limit up to which data might be collected, the take-it-or-leave-it nature of consent notices might defeat the purpose of such protection measures and jeopardise the interests of consumers.

It has been suggested that the goals of consumer welfare can only be truly met by taking into account growing risks and unsatisfactory preferences with regard to privacy through disproportionate accumulation of data or discriminatory terms and conditions. For this approach to work, it is necessary that privacy be viewed within the framework of a parameter alongside price factors. In this way, harmful impacts on privacy would be as apprehensible for competition stakeholders as predatory pricing or repressed innovation.

CCI has further apprehended that practices such as the ones by Facebook under probe could work to further retrench their positions in respective or even related markets. This may be reflected in the potential exclusionary effects in the display advertising market as a result of the provision of direct data sharing under the garb of consumer profiling (CCI Suo Moto Case No. 01, 2021)

Traditionally, the overlap in the ultimate goals of competition law and data protection has been ignored, as seen in the separate rules and regulations applied distinctly, but the time is now ripe to recognise that a particular issue might require perspectives from both spheres. There is enough room for laws to be applied coherently without one going beyond its scope and impinging on another. Competition law can act to render the operation of data protection more effective.

Competition law will have to work in harmony with data protection and consumer welfare systems, since regulating the dominant behaviour of platforms as far as exploitation of users is concerned constitutes an indispensable mandate (Kerber & Zolna, 2021). This will be a necessity in the future since, in the digital era, where data is the price that consumers pay for services, abuse of dominance is more likely to result in unreasonable terms and conditions than skyrocketing prices (Buiten, 2020). Another perspective on this issue could be that dominant firms, for the very reason that they hold enormous control in the market, should be deployed with a special responsibility to ensure that their conduct does not hamper

the environment of thriving competition (*Nederlandsche Banden Industrie Michelin v. Commission*, 1983).

In order to overcome the challenges of antitrust issues underlying the data privacy lacuna, competition authorities would have to broaden their vision and tools to scrutinise anti-competitive effects. Given the dangers of concealed data practices and the privacy paradox, authorities need to be cognizant of the preferences of users to determine whether customers are conscious of data protection within a given market. This would become relevant when data mergers create possibilities of data sharing.

There needs to be a thorough analysis of privacy policies to detect whether they involve practices which take users' preferences hostage or whether circumstances with possible exclusionary effects could improve privacy. This also calls for a detailed empirical accounting of competition on privacy, which could be furthered by relevant data shared by data giants, who are often reluctant to do so. Antitrust authorities ought to incentivise data giants in order for the data to become more accessible and available to be assessed by statistical and academic experts (Blankertz, 2020).

This would also be effective in designing a framework which addresses the accumulation of power based on data in the data giant's ecosystem, locating potential asymmetries in scale and scope between the dominant player and other players, and analysing possible entry barriers for competitors that could be created in the face of exclusive information under possession of the data giant (Hoffmann & Johannsen, 2019).

The increasingly complex issues in digital markets have a better chance at comprehensive scrutiny if they receive the cooperative analysis of privacy (when established) and competition authorities given the potential for flow of information and joint discussions. This could result in efficient assessment of the central issue and formulating strategies and procedures that could work in combination. Such collaborative policies could set the paradigm for consumer choice. However, one needs to be mindful of the fact that competition law cannot be considered a substitute for data protection law, especially in India, which is still awaiting the enactment of a legislation that is built vigorously to address issues of privacy.

References

Arthur, C. (2021) Tech giants may be huge, but nothing matches big data. *The Guardian*. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data

Balto, D.A., & Lane, M. (2016). *Monopolizing water in a tsunami: Finding sensible antitrust rules for big data*. https://doi.org/10.2139/ssrn.2753249

Blankertz, A. (2020). *How competition impacts data privacy*. https://www.stiftung-nv.de/sites/default/files/how_competition_impacts_data_privacy.pdf

Buiten, M.C. (2019). Regulating data giants: Between competition law and data protection law. *Springer International Publishing*. https://doi.org/10.1007/978-3-030-11611-8_13

Buiten, M.C. (2020). Exploitative abuses in digital markets: Between competition law and data protection law. *Journal of Antitrust Enforcement*, *9*(2), 270–288. https://doi.org/10.1093/jaenfo/jnaa041

Bundeskartellamt. (2019). *Administrative proceedings decision under Section 32(1) German Competition Act (GWB)*. http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf%3F__blob%3DpublicationFile%26v%3D5

Bundeskartellamt. (2019). *Bundeskartellamt prohibits Facebook from combining user data from different sources*. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

Bundeskartellamt v. Facebook Inc., Federal Court of Justice Decision KVR 69/19

Bundeskartellamt. (2016). *Bundeskartellamt initiates proceeding against Facebook on suspicion of having abused its market power by infringing data protection rules*. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html

Competition Act, 2002, Act No. 12 of 2003. https://doi.org/10.1016/S1361-3723(02)00226-9

Competition Commission of India Case No. 15 of 2020

Competition Commission of India Suo Moto Case No. 01 of 2021

Complaint under Article 77(1) GDPR. https://noyb.eu/sites/default/files/2020-05/complaint-facebook.pdf

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

European Commission. (2017). *Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover*. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369

Ezrachi, A. & Robertson, V. H.S.E. (2019). Competition, market power and third-party tracking. *World Competition: Law and Economics Review, 42*, 5–19. https://doi.org/10.54648/WOCO2019002

Facebook/Bundeskartellamt. The decision of the higher regional court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings (2019) Case VI-Kart 1/19 (V)

Graef, I., Clifford, D. & Valcke, P. (2018). Fairness and enforcement: bridging competition, data protection, and consumer law. *International Data Privacy Law. 8*(3), 200–223. https://doi.org/10.1093/idpl/ipy013

Gupta V.K. & WhatsApp Inc., Case No. 99 of 2016

Hoffmann, J. & Johannsen, G. (2019) EU-merger control & big data on data-specific theories of harm and remedies. *Max Planck Institute for Innovation and Competition Research Paper Series*.

Hogben, G. (Ed.). (2007). Security issues and recommendations for online social networks. *Enisa Position Paper No. 1.*

IFF. (2021). Big opportunity! CCI accepts IFF's expert information in its investigation of WhatsApp's 2021 privacy policy. *Internet Freedom*. https://internetfreedom.in/big-opportunity-cci-accepts-iffs-expert-information/

Kemp, K. (2020). Concealed data practices and competition law: Why privacy matters. *European Competition Journal, 16*(2–3), 628–672. https://doi.org/10.1080/17441056.2020.1839228

Kerber, W. & Zolna, K. K. (2021). *The German Facebook case: The law and economics of the relationship between competition and data protection law*.

https://www.ucl.ac.uk/laws/sites/laws/files/kerber_zolna_2021_facebook_case_competition_law_data_protection_law_01.pdf

Kimmel, L. & Kestenbaum, J. (2014). What's up with WhatsApp: A transatlantic view on privacy and merger enforcement in digital markets. *Antitrust, 29*(1).

Lee J. (2020). The Google-DoubleClick merger: Lessons from the Federal Trade Commission's limitations on protecting privacy. *Communication Law and Policy*.

Mal, A. & Parikh, J. (2011). Facebook and the right to privacy: Walking a tight rope. *Nujs Law Review, 4*, 299.

Mehmood, A. (2016). Protection of big data privacy. *IEEE Access, 4*, 1821–1834. https://doi.org/10.1109/ACCESS.2016.2558446

Moshell, R. (2005). And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework. *Texas Tech Law Review, 37*, 357.

Nederlandsche Banden Industrie Michelin v Commission, Case 322/81, ECLI:EU:C:1983:313

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. https://doi.org/10.1515/9780804772891.

Niu, E. (2016) European regulators are mad at Facebook and WhatsApp over sharing data. *Business Insider*. https://www.businessinsider.com/Facebook-Whatsapp-European-Regulators-Data-Sharing-2016-12?Ir=T

OECD. (2020). *Abuse of dominance in digital markets*. www.Oecd.Org/Daf/Competition/Abuse-Of-Dominance-In-Digital-Markets-2020.Pdf

Personal Data Protection Bill (2019) Bill No. 373 of 2019

Puttaswamy, K.S. & Anr. v. Union of India & Ors. (2017). 10 SCC 1

Statement of FTC concerning Google/DoubleClick FTC File No. 071-0170. https://www.Ftc.Gov/System/Files/Documents/Public_Statements/418081/071220googledc-Commstmt.Pdf

Stojanovic, M. (2020). Can competition law protect consumers in cases of a dominant company breach of data protection rules. *European Competition Journal, 16*, 531–569. https://doi.org/10.1080/17441056.2020.1824464

Stucke, M. & Grunes, A. (2016). *Big Data and Competition Policy*. OUP.

Valetti, T. (2019). Testimony of Tommaso Valetti, Ph.D. Professor of Economics Imperial College Business School, Imperial College London, before the House Judiciary Committee Subcommittee on Antitrust, Commercial, and Administrative Law on Online Platforms and Market Power Part 3: The Role of Data and Privacy in Competition

Van den Bergh, R. & Weber, F. (2021). The German Facebook saga: Abuse of dominance or abuse of competition law? *World Competition Law and Economics Review, 44*(1), 29–52. https://doi.org/10.54648/WOCO2021003

Wahyuningtyas, S. Y. (2017). Abuse of dominance in non-negotiable privacy policy in the digital market. *European Business Organization Law Review, 18*(4), 785–800. https://doi.org/10.1007/s40804-017-0084-0

Wasastjerna, M.C. (2019). The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface. *European Business Law Review, 30*(3), 337–365. https://doi.org/10.54648/EULR2019017

WhatsApp and Facebook to share users' data outside Europe and UK. (2021). *BBC.* https://www.Bbc.Com/News/Technology-55573149, Retrieved 15 November 2021

WhatsApp. (2016). *New features for more privacy, more protection, more control.* https://blog.whatsapp.com/looking-ahead-for-whats-app, Retrieved 27th July 2022

WhatsApp LLC v. Competition Commission of India & Anr, AIR 2021 (NOC 710) 281

WhatsApp Privacy Policy. (n.d.) https://www.Whatsapp.Com/Legal/Updates/Privacy-Policy/?Lang=En