CENTRE FOR ACADEMIC LEGAL RESEARCH | JOURNAL OF APPLICABLE LAW &JURISPRUDENCE

Volume 1 | Issue 1

"Facebook's Monopoly and Data Protection: A Closer Look"

By: Vaishali Pooniwala (G D Goenka University)

ABSTRACT

Facebook has been sued by FTC allegedly for abuse of its dominant position and creating a monopoly in the social media market. However, it is not the only thing that Facebook is violating. Data Protection is one of the important aspects of Competition Law and Human Rights, and it is high time to regulate the Data protection and Activities of Facebook.

INTRODUCTION

The World is recovering from a serious disease, the Global Pandemic of "CoVid-19". While the world was disconnected, the only thing which kept us connected, entertained, and informed during the quarantine was social networking. People during quarantine made and watched videos on recipes, art, and it was all possible because of the huge network of social media available to us on our smartphones. Social media is a hub of technology that facilitates the creation and sharing of information, ideas, and other forms of communications among the virtual community. One such widely known Social media platform is Facebook, a company founded in a dorm room by few Harvard students. It is an online application, connecting users to their friends and family, to share videos, photos, exchange status, messages, etc. The popularity of Facebook is evident by the growth of its userbase since its inception in 2004, which increased from 1m to 2.45bn till 2019.[1] However, Facebook is not the only popular app. Applications like Instagram, Snapchat, Tik Tok, YouTube have wooed users with their video-photo sharing features. WhatsApp for instance has not only made its place in our day-to-day mobile usage but has efficiently replaced the in-built messaging facilities provided by the mobile network operators.

Facebook in 2012 purchased Instagram for $1bn and WhatsApp in 2014 for $19bn[2], making Facebook a company owing to the 4 most used apps of the decade. Federal Trade Commission (FTC), America sued Facebook on 9 December 2020 alleging that the company is maintaining its personal social networking monopoly by anti-competitive conduct. The complaint was based on the finding of an investigation done by the attorney generals of 46 states, The District of Columbia and Guam, which states that Facebook has engaged in systematically acquiring its rival companies (Instagram/WhatsApp) and imposed anti-competitive threats to eliminate the threats to monopoly. On the stated grounds, the FTC has sought for permanent injunction which may require divestitures of assets and prior permission for future mergers and acquisitions.[3] Similarly in 2018 Facebook was accused of anti-competitive behavior by

---

[1] Felix Richter, Facebook Keeps on Growing, Statista, https://www.statista.com/chart/10047/facebooks-monthly-active-users/, (Nov. 1, 2019).

[2] Sam Shead, BBC News, Facebook owns the four most downloaded apps of the decade, https://www.bbc.com/news/technology-50838013, (Dec. 18, 2019).

[3] FTC, FTC Sues Facebook for illegal monopolization, https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization (Dec. 9, 2020).

weaponizing user data to gain an advantage over competitors[4] and in January 2020, the app developers complained over Facebook's anti-competitive conduct[5].

In response to FTC's claim, Facebook stated that the acquisition of Instagram by Facebook has been approved by FTC itself, and so has the acquisition of WhatsApp by the European Union, therefore, pursuing the case would render risk on completion of any sale.[6]

However, it is highly pertinent to prioritize the interest of the public at large, as even though Facebook was earlier cleared from the charges of anti-competitive behavior, much later it was realized that the actions were more of anti-competitive conduct of Facebook. Vine, a video creation and streaming app introduced by Twitter, faced failure, because Facebook did not provide access to "friends" on Facebook, similarly Facebook tried to purchase Snapchat, on the failure of which Facebook introduced the exclusive famous feature of Snapchat known as "story" on its platforms as well.

This kind of anti-competitive policy not only deprives the consumers of personal social networking, as everything is being accessed through Facebook but also makes it easier for Facebook to hinder the Data protection laws, because of the absence of challenge in the market on its quality of privacy protection provided.

WHAT IS DATA PROTECTION AND WHY IS IT NECESSARY?

In Data protection the data and the important pieces of information are safeguarded from any kind of wrongful loss, compromise, or corruption. However, in the legal language, it refers to the set of privacy rules, policies, and procedure which focuses on minimizing the intrusion to one's privacy caused by the collection, storage, and distribution or transfer of data especially Personal data.[7]

Personal data refers to such information relating to individuals through which the person can be identified, either collected by Government or private organization or agency, it includes,

---

[4] Hannah Kuchler, Financial times, Facebook accused of anti-competitive behaviour, https://www.ft.com/content/a383ab46-5f6b-11eb-9334-2218e7146b04 (May 24, 2018)

[5] Bloomberg, The Economic Times, 4 tech cos sue Facebook for anti-competitive behaviour, https://m.economictimes.com/tech/internet/4-tech-cos-sue-facebook-for-anti-competitive-behaviour/articleshow/73349236.cms (Jan. 18, 2020).

[6] Cecilia Kang & Mike Issac, N.Y. Times, U.S. and States Say Facebook Illegally Crushed Competition https://www.nytimes.com/2020/12/09/technology/facebook-antitrust-monopoly.html (Dec. 9, 2020).

[7] Vijay Pal Dalmia, Mondaq, Data Protection Laws in India: Everything You Must Know, https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know (Dec. 13, 2017)

date of birth, name, email id, biometrics, or other such characteristic details.[8] The data is required to relate to the data subject and to be collected and processed by the data controller. It may or may not be unique to the subject but should be enough for identification.[9] Right to Data Protection is not explicitly recognized anywhere, however it comes under the umbrella of Right to Privacy, which the Courts have ruled under the domains of Right to life and personal liberty under Article 21 under the Constitution of India. In *Justice K.S. Puttayswamy (Retd.) & Anr. v. Union of India & Ors.*[10] the Constitution bench of Hon'ble Supreme Court recognized the Right to Privacy as a fundamental right, subject to certain reasonable restrictions. The protection of personal data is therefore not only important for the person's identity but for the effective realization of the fundamental rights and freedoms of the individuals related to data. Non-compliance can lead to identity theft or life-threatening situations.[11]

The phrase 'Data is the new oil' has taken another dimension as data is becoming valuable, and it is clear from the fact that Amazon, Google, Apple, Microsoft, and Facebook, the five most valuable companies currently in the world, the giants belong to the data industry. With time the skills of handling and retrieving personal data are evolving very fast, but the legislations are yet to catch up with the speed. The importance of data protection increases with the increase in the unprecedented rate at which the data is being created and stored.

Data protection is also necessary to ensure fair and consumer-friendly commerce and services, as personal data without any regulations can be sold freely depriving people the power to take the stand. In Facebook/WhatsApp[12] case itself European Commission pointed out that Data privacy policies constitute a parameter of competition, as it can affect the product quality and price paid by the consumer in terms of the requirement of data to be provided. In several other cases like Microsoft/LinkedIn[13] and Google/DoubleClick[14], EC and USFTC have respectively observed that data protection is one of the key factors of quality in professional social networks, moreover, consumer privacy can get adversely affected by mergers. In case if a company tries to collectively lower the degree of privacy provided, it would result in anti-competitive practice

---

[8] *Id.*
[9] Global Partners Digital, Travel Guide to The Digital World: Data Protection for Human Rights Defender, https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf.
[10] 10 SCC 1 (2017).
[11] Katrine Sarap, NJord Law Firm, Three Reasons Why We Need Strict Data Protection Regulations, https://www.njordlaw.com/three-reasons-why-we-need-strict-data-protection-regulations, (Oct. 9, 2018).
[12] Eleonora Ocello, Cristina Sjödin & Anatoly Subočs, What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case, Competition Merger brief (Feb., 2015)
[13] Microsoft/LinkedIn Case, (COMP/M.8124), European Commission, 2016.
[14] Statement of the FTC Concerning Google/DoubleClick, File no. 071-0170, USA, 2007.

or competitive advantage of providing poor quality of service overall, which is straight-out, not possible, whereas acquiring the company and its data by being in the dominant position does the work. Facebook through introducing new policies as seen in 2021 will acquire not only access to its users who explicitly use or used Facebook but also access to the data of users of WhatsApp and Instagram as well. As observed by the Competition Commission of India in Sou-moto Case 1 of 2021, the new policy of WhatsApp which makes it compulsory for the user to accept the continued services of WhatsApp is the permission to share user data to its Parent Company, i.e. Facebook. In this context, it is relevant to note that Facebook and WhatsApp have a dominant position in the market as observed by the Commission in *Harshita Chawla Case*, where the commission concluded that WhatsApp being the Over-the-Top service provider has a direct network advantage, so for a user to connect to another person, the person should have to be on the same network, and therefore the user cannot leave the platform as the person would leave the social connectivity in its consequence.

As it was observed just after the notification of the update of the new WhatsApp policy, 2021, the users started to switch to Signal and Telegram yet WhatsApp did not lose any significant amount of its userbase. Further WhatsApp and Facebook belonging to the same group add-ons to their advantage, and the given popularity with unique features gives the applications a dominant position.

By virtue of this Facebook is able to abuse its dominant position in several ways, as noted in the case of the vine, and other such third-party developers who denied compliance with Facebook were, in turn, denied the access of user data which was necessary for the functioning of the app, or for the budding businesses to enter into the market.[15] Hence, the practice is also hindering the advertisers from attaining the potential advantage of competition, due to the lack of choices available.

When in 2016 WhatsApp introduced a similar cross-platform data sharing policy, WhatsApp gave an option to the users to opt-out from the said update which would share their information with the Facebook group, against which in *Vinod Gupta Case*, it was alleged that the data which will be acquired by Facebook is going to be used for targeted advertising which is against the competition policy, on which the Commission observed that the company provided the opt-out option which makes the update in consonance with competition policy. However, the same is

[15] Hannah Kutcher, Facebook accused of 'anti-competitive' behaviour, available at https://www.ft.com/content/a383ab46-5f6b-11e8-9334-2218e7146b04 (May 24, 2018).

missing from the update of 2021. Moreover, the expressions used by Facebook in the terms of services FAQ about the update are vague, such as information on how users interact with each other (including business), service-related information, payment-related information, etc leading to an open-end and incomplete disclosures. The policy update, therefore, attracts the attention of CCI under Sec 4(2)(c) and (e) on the grounds of degrading quality and creating barriers for the new potential business in both data and advertisement sector.

Similar acquisitions have been pressed under European Union's DPA where the new policy is being scrutinized for being against the data privacy policies of the European Union General Data Protection Regulations.

Under competitive conditions, the users must have complete control over decisions on sharing their personalized data, as the consent asked by Facebook is neither voluntary nor transparent. The users moreover should also have all the information on how their data is to be used by a company, however, one of the listed purposes for the data sharing in cross-platform is targeted advertising, that is to create a profile of users and to advertise products and services as per their profiles. This in itself is a competitive advantage to the data-bearing companies resulting in an anti-competitive practice. The data sharing among the cross-platform results in degradation of non-pricing parameters of competition, that is the quality of service provided to users. With the reduction of user's capability of control on their sensitive data and quality of data protection, the users are on verge of getting exploited, such actions further entrench an unrelated market of advertisement through targeting.

The abuse of dominance is not only affecting the free market, and free choice of consumers and advertisers, but is also helping Facebook, and other such tech giants to exploit their dominant position in terms of user data and manipulate behavioral advertisement, by monitoring the behaviors of user's online. The behavioral targeting is done by cookies, through which profiles of internet users are compiled in details, the data of cookies is based on what the user read, watches, search and like, etc. Such characteristic likes of the person get recorded in a small packet of data which can be accessed by first-party applications as well as third-party applications, arising the privacy concern. When an internet user visits a website, advertising networks, serving advertisements on the website can recognize the user using these cookies. In most of the Laws[16], the processing of personal data is required to be done for legitimate purposes, only after obtaining the consent of the user. Therefore, when the cookies are used for

[16] Charter of Fundamental Rights of European Union, 2009 (EU).

remembering the contents of the shopping cart, it can be proven with the legitimate purpose principle.

However, the companies engaged in behavioral targetings, such as Facebook, Google, can generally tie the names and email addresses of their users with the data of individuals. Email service providers can link the email addresses, and as well analyze communications made by the user for behavioral targeting.[17] The profile sets can be made extremely detailed for more personality profiling. The same has to be reviewed under the Data Protection Law, as the packet of data contains the data which enables the data subjects to be singled out[18] by detailed personality profiling which can not only help in manipulation of consumer behavior but may also help the companies engaged in behavioral advertising manipulate consumer choices in a free market. In such cases users are allowing that their data to be accessed for their own manipulation by the way of algorithms, Therefore, when we search about Puppies, we end up getting tons of advertisements of Puppy adoption facilities, food, etc.

Such manipulation tactic was also noted during the time of the US election when the company named Cambridge Analytica collected data from Facebook, and the incident is considered one of the largest Facebook data leaks. Cambridge Analytica aimed to persuade with the personalized advertisement presented to people, predicting their personality based on data collected through the Facebook page likes of the users, and to make them vote in a certain way. However, the company which sourced the personality data for Cambridge Analytica broke the terms of service of Facebook and was resultantly asked to delete all Facebook data in 2015. The procedure used by the source company was based on a survey that asked the respondents about their personality traits using a third-party survey provider. The survey asked the participants to provide consent to access the Facebook data, including the pages they liked, which also gave the company access to the details of page likes of the participant's friends, who had not disabled the certain set of security on Facebook. Consequently, the company collected data of around 30m users, on the basis of 2,70,000 participants of the survey. The

[17] Gmail Ads help, 'Ads in Gmail. How Gmail Ads work' available at https://support.google.com/google-ads/answer/7019460?hl=en#:~:text=Gmail%20ads%20are%20interactive%20ads,%2C%20video%2C%20or%20embedded%20forms.

[18] Frederik Zuiderveen Borgesius, Consent to Behavioural Targeting In European Law - What Are The Policy Implications Of Insights From Behavioural Economics?, Amsterdam Law School Legal Studies Research Paper No. 2013-43.

data was then processed to make the details of the personality traits of users, although it was deleted before the US 2016 election.[19]

However, such leaks raise concern on how protected our personal Data is, and is Behavioural Targeting adequately regulated under Data Protection bills, present as of now. The processed data of users is exploited to profile them such that, not only product advertisement can be customized, but the political and polarization agenda can be furthered, it includes foreign intervention in the election to target campaigns, focusing on confusing and dividing users on important social issues based on their personalities and appeal. The messages presented to us are not all advertisements, and such features can be used to amplify, racial harassment, hate speech, and other such radicalizing elements.[20] Profiling the people for the purpose of manipulating them for elections also goes against the spirit of democracy and the right to vote and choose a government.

Facebook having a dominant position in the market, purchases other such tech giants, which possess lots of user data. It is not only dangerous to Free market policies and Competition law, but also to the data privacy of the concerned users. As the quote goes "If you're not paying for it, you are the product".[21] We pay with our personal data, to use internet services, but at the cost of getting targeted. This same targeting is also a threat to democracy as we know it.[22]

PERSONAL DATA PROTECTION REGULATIONS AT PRESENT

INTERNATIONAL

The first data protection bill was passed by the German Federal State of Hesse in 1970[23], the world has made significant progress from the time as in 2018 itself, European Union's General

---

[19] Rahul Rathi, Effect of Cambridge Analytica's ads on 2016 US Presidential elections, available at https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d (Jan. 13, 2019).

[20] Pierre Omidyar, Disinformation and social media: six ways in which social media pose threat to transparency and democracy, available at https://economictimes.indiatimes.com/news/politics-and-nation/disinformation-and-social-media-six-ways-in-which-social-media-pose-a-threat-to-transparency-and-democracy/articleshow/61128404.cms (Oct. 18, 2017).

[21] Scott Goodson, If you're not paying for it, you become the product, available at https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/ (Mar. 8, 2012)

[22] Kalev Leetaru, A Reminder that social media platforms are now the greatest threat to democracy, available at https://www.forbes.com/sites/kalevleetaru/2019/04/25/a-reminder-than-social-media-platforms-are-now-the-greatest-threat-to-democracy/?sh=e9e22d07c7d3 (Apr. 25, 2019,)

[23] *Supra* at *note* 9.

Data Protection Regulation (GDPR) took effect, aiming to harmonize data protection and privacy requirements in EU. Similar data protection regulations are being implemented or are in process of implementation, for instance in the USA a bill has been proposed to expand the criminal liability to the executives of the companies that suffer data breaches.[24]

The GDPR is the strictest privacy and security law at present. It entered into force in 2016, the scope of GDPR extends to all organizations which process personal data of EU citizens or residents or offer goods or services to such people. The fine for non-compliance with GDPR is of two tiers which extend to €20 Million or 4% of global revenue whichever is higher, plus the data subjects have the right to seek compensation for the damages. The Data protection principle necessary as per GDPR is enshrined under Article 5.1.2[25] which is

(1) The processing of data must be lawful, fair, and transparent to the data subject,
(2) The processing should be for legitimate purposes specified explicitly to the data subjects,
(3) Only absolutely necessary data for the specified purpose should be collected and processed,
(4) Personal data should be accurate and updated,
(5) Data should only be stored for as long as it is necessary for the specified purpose,
(6) Processing must ensure security, integrity, and confidentiality,
(7) The data controller is responsible to demonstrate compliance with GDPR.

GDPR in its Article 6[26] also specifies the conditions where the processing of Data is legal, it includes data for which the data subject has given unambiguous consent, or is necessary for the execution of the contract to which data subject is part, or to comply with a legal obligation such as order of the court, to save somebodies life, to perform a task in the public interest or for any other legitimate interest. However, Data subjects can withdraw the consent whenever they want to.

GDPR being tough legislation provides for multiple privacy rights for data subjects such as the data subject has a right to be informed about who is using data and for what purposes inclusive of other necessary information.

---

[24] GDPR, EU, What is GDPR, The EU's New Data Protection Law, https://gdpr.eu/what-is-gdpr/
[25] (EU) 2016/679, OJ 2016 L 119/1, 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), (Apr. 27, 2016).
[26] *Id.*

Right to Erasure as individuals have a right to request that their data be erased provided that certain grounds apply.

Other rights guaranteed under GDPR are the Right to access, right to rectification, right to restrict processing, right to data portability, right to object, etc.

INDIA

India although does not have as of yet the legislation on Data protection except for the Information Technology Act, 2000 and IT Rules, 2011[27] which does entrust certain safeguard and control to Government in regulating data and information over the internet under Section 69A[28], and to penalize body corporate and individuals for compromising data under Section 43A and 72A[29], however it is not enough, as IT Act was not enacted with the primary intent of data protection and therefore, its scope is limited. Thereby, India is in process of implementing the legislation satisfying the same requirements. Inspired by GDPR[30], the Draft Personal Data Protection bill[31] was proposed in 2019. The bill proposes the compliance requirements for personal data of all types, it expands the rights given to individuals, institute central data protection regulator, and data localization of sensitive information and data requirements. It is applicable to non-Indians organizations extra-territorially as well when certain requirements are met, and imposes hefty financial penalties on non-compliance.

The PDP Bill promises to bring major reforms in the Data Protection domain, however few of the most promising are the following;

Health Data: IT Rules only protected limited set of information such as physical, mental, physiological conditions, sexual orientation, medical record, and history, however, the uncovered part of health data also comprises different information's including patient details, contacts, reports, digital health records, which is highly valuable for healthcare industries. It also includes information being recorded in fitness apps or gadgets like Fitbit, Apple fitness, etc, or the online health information, or information filled in online free diagnostic services. The compliance under the IT Rules is limited to obtaining consent for the collection, tor transfer

[27] Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R. 313(E), (Apr. 11, 2011).
[28] Information Technology Act, 2000, Act 21 of 2000, (Oct. 17, 2000).
[29] *Id.*
[30] *Supra* at *note* 25.
[31] Personal Data Protection Bill, Bill 373 of 2019.

of personal data along publishing privacy policy, but the organizations are not made liable to inform the users about any data breach for their health records.

The PDP Bill addresses the same by proposing the data breach notification mandatory, with data breaches being punishable with a fine and imprisonment up to 5 years

Geo-Location Information is not included by the IT Rules under sensitive personal data and therefore, organizations are not liable for disseminating such information to other parties. Most of the mobile applications or smartwatch applications such as Facebook, Google, Life360 track the locations of their users while using or not using the app. Without any strict penal provisions of liability, the apps can easily trade the location information with a third party. PDP bill addresses the same as it proposes a wider definition of personal data which includes the Geo-Location information and increased applicability of inclusion of processing personal data by any organization whether Government, private or foreign.

Right to be Forgotten: Just like as enshrined in Article 17 of GDPR individuals will have the right to have their personal information removed from any public domain. The right to be forgotten has been recognized by the Supreme Court to fall under the ambit of Article 21 of the Constitution of India.[32] Interestingly it originated when Mario Costeja sued Google for the removal of a 1998 newspaper article which stated a negative notion about him on the grounds that it was no more relevant, when Google denied the request, he approached the European Court of Justice, which ruled in his favor.

The PDP Bill on the same basis proposes that individuals would be able to limit, delete, delink or correct any misleading embarrassing, and irrelevant information.

As the new PDP Bill promises a lot of reforms in the Data Protection regime in India, it needs to be implemented at the soonest, as the internet world is ever-changing and by taking the first step at least the basics will be regularised.

The PDP Bill also needs to impose hefty penalties on giant multinationals such as Facebook and its subsidiaries, Google, etc., for non-compliance so that the purpose of regularization can be properly served.

After successful implementation of the same, further, the authorities should dwell to regulate the Behavioural Targeting and its aspects in accordance with the Data Privacy and Protection

[32] *Supra* at *note* 10.

law, all the data which is irrelevant or which can be used for behavioral targeting should be regularised, the collection and transfer of such data should be informed to the data subject.[33]

Furthermore, Mergers and Acquisitions of Tech giants like Facebook should be scrutinized strictly, not only on the terms of market share, or available provisions of the Competition Law. Considering these companies gain profit with the data of users they gain, and by not exactly manipulating the prices, it is pertinent to note, observe and predict how the acquisition of such companies, with other wide user-base companies, will have what kind of effect on personal data of users, and how will it be used in furtherance of their policies.

[33] ICO, Right to erasure, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#:~:text=The%20right%20to%20erasure%20is,to%20respond%20to%20a%20request.&text=This%20right%20is%20not%20the,whether%20to%20delete%20personal%20data.

CONCLUSION

Facebook with such a vast repository of personal data of most of the world population is as dangerous as an irresponsible country possessing nuclear power. User data accessed by anyone for illegitimate and illegal purposes will be no less than a digital nuclear bomb, endangering the personal details of multiple users. Letting Facebook create a monopoly over the social networking market is, therefore, hindering the innovations waiting to happen in relation to data protection, and thus it is high time that Facebook must be regulated properly.

The contemporary competition act is so made to prevent such agreements in brick and mortar which may result in anti-competitive practices, but with the growing digital realm age, it does not completely address the issue of Data protection of users with respect to anti-competitive practices. The tech giants while merging may not transact in cash as much to attract the anti-competitive law but certainly, they trade in data of users which is equivalent to the cash for these companies.

Moreover, with increasing awareness of Rights related to the protection of personal data, as seen during February 2021 when WhatsApp introduced its new privacy policy facing outrage of people, resulting in Facebook in delaying the same, it is high time to assure individuals by bringing 'relevant to time' legislation for the regulation of data protection, that their data is safe.[34]

As rightly said, "Data is the pollution problem of the information age, and protecting privacy is an environmental challenge" (Bruce Schneir), it is high time for sustainable development.

[34] Jagmeet Singh, Gadget 360, WhatsApp: Everything You Need to Know About the Controversial Privacy Policy Update, https://gadgets.ndtv.com/apps/news/whatsapp-privacy-policy-update-changes-what-happens-if-you-dont-agree-details-facebook-data-2376020, (Feb. 22, 2021).

Researcher/Scholar Index

- [1] Felix Richter, Facebook Keeps on Growing, Statista, https://www.statista.com/chart/10047/facebooks-monthly-active-users/, (Nov. 1, 2019).
- [1] Sam Shead, BBC News, Facebook owns the four most downloaded apps of the decade, https://www.bbc.com/news/technology-50838013, (Dec. 18, 2019).
- [1] FTC, FTC Sues Facebook for illegal monopolization, https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization (Dec. 9, 2020).
- [1] Hannah Kuchler, Financial times, Facebook accused of anti-competitive behaviour, https://www.ft.com/content/a383ab46-5f6b-11eb-9334-2218e7146b04 (May 24, 2018)
- [1] Bloomberg, The Economic Times, 4 tech cos sue Facebook for anti-competitive behaviour, https://m.economictimes.com/tech/internet/4-tech-cos-sue-facebook-for-anti-competitive-behaviour/articleshow/73349236.cms (Jan. 18, 2020).
- [1] Cecilia Kang & Mike Issac, N.Y. Times, U.S. and States Say Facebook Illegally Crushed Competition https://www.nytimes.com/2020/12/09/technology/facebook-antitrust-monopoly.html (Dec. 9, 2020).
- [1] Vijay Pal Dalmia, Mondaq, Data Protection Laws in India: Everything You Must Know, https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know (Dec. 13, 2017)
- [1] *Id*.
- [1] Global Partners Digital, Travel Guide to The Digital World: Data Protection for Human Rights Defender, https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf.
- [1] 10 SCC 1 (2017).
- [1] Katrine Sarap, NJord Law Firm, Three Reasons Why We Need Strict Data Protection Regulations, https://www.njordlaw.com/three-reasons-why-we-need-strict-data-protection-regulations, (Oct. 9, 2018).
- [1] Eleonora Ocello, Cristina Sjödin & Anatoly Subočs, What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case, Competition Merger brief (Feb., 2015)
- [1] Microsoft/LinkedIn Case, (COMP/M.8124), European Commission, 2016.
- [1] Statement of the FTC Concerning Google/DoubleClick, File no. 071-0170, USA, 2007.
- [1] Hannah Kutcher, Facebook accused of 'anti-competitive' behaviour, available at https://www.ft.com/content/a383ab46-5f6b-11e8-9334-2218e7146b04 (May 24, 2018).
- [1] Charter of Fundamental Rights of European Union, 2009 (EU).
- [1] Gmail Ads help, 'Ads in Gmail. How Gmail Ads work' available at https://support.google.com/google-ads/answer/7019460?hl=en#:~:text=Gmail%20ads%20are%20interactive%20ads,%2C%20video%2C%20or%20embedded%20forms.
- [1] Frederik Zuiderveen Borgesius, Consent to Behavioural Targeting In European Law - What Are The Policy Implications Of Insights From Behavioural Economics?, Amsterdam Law School Legal Studies Research Paper No. 2013-43.
- [1] Rahul Rathi, Effect of Cambridge Analytica's ads on 2016 US Presidential elections, available at https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d (Jan. 13, 2019).
- [1] Pierre Omidyar, Disinformation and social media: six ways in which social media pose threat to transparency and democracy, available at https://economictimes.indiatimes.com/news/politics-and-nation/disinformation-and-social-media-six-ways-in-which-social-media-pose-a-threat-to-transparency-and-democracy/articleshow/61128404.cms (Oct. 18, 2017).
- [1] Scott Goodson, If you're not paying for it, you become the product, available at https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/ (Mar. 8, 2012)
- [1] Kalev Leetaru, A Reminder that social media platforms are now the greatest threat to democracy, available at https://www.forbes.com/sites/kalevleetaru/2019/04/25/a-reminder-than-social-media-platforms-are-now-the-greatest-threat-to-democracy/?sh=e9e22d07c7d3 (Apr. 25, 2019,)
- [1] *Supra* at *note* 9.
- [1] GDPR, EU, What is GDPR, The EU's New Data Protection Law, https://gdpr.eu/what-is-gdpr/
- [1] (EU) 2016/679, OJ 2016 L 119/1, 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), (Apr. 27, 2016).
- [1] *Id.*

- [1] Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R. 313(E), (Apr. 11, 2011).
- [1] Information Technology Act, 2000, Act 21 of 2000, (Oct. 17, 2000).
- [1] *Id.*
- [1] *Supra* at *note* 25.
- [1] Personal Data Protection Bill, Bill 373 of 2019.
- [1] *Supra* at *note* 10.
- [1] ICO, Right to erasure, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#:~:text=The%20right%20to%20erasure%20is,to%20respond%20to%20a%20request.&text=This%20right%20is%20not%20the,whether%20to%20delete%20personal%20data.
- [1] Jagmeet Singh, Gadget 360, WhatsApp: Everything You Need to Know About the Controversial Privacy Policy Update, https://gadgets.ndtv.com/apps/news/whatsapp-privacy-policy-update-changes-what-happens-if-you-dont-agree-details-facebook-data-2376020, (Feb. 22, 2021).