FREE SERVICES OR PRIVACY: FORMULATING THE CHOICE FOR CONSUMERS IN ZERO-PRICE MARKETS

— *Pankhudi Khandelwal*[*]

Abstract: *Zero-priced markets have become important in the present digital society. The revenue models of Facebook and Google use targeted advertising for revenues. Based on this, it can be argued that zero-priced products are not free as consumers 'pay' in form of attention to these advertisements. Zero-priced markets have the potential to be harmful for the consumers in form of less privacy. While the data protection law deals with the protection of personal data, however, this data is acquired by the companies on the basis of consent, performance of a contract or legitimate interests.*

Most consumers are either not aware about how their data is being used or do not value their data enough to give up the zero-priced services. In light of this changing technological environment, the article suggests whether this choice should be made on behalf of the consumers through regulation under the consumer welfare standard whereby companies are either required to change their current business model or provide for better provisions for privacy. The article aims to provide an improved legal framework of competition law, consumer protection law and data protection law to provide a balance in regulating digital markets.

Keywords: Consumer Protection, Competition Law, Consumer Welfare, Data Protection, Privacy, Zero-priced, etc.

[*] Pankhudi Khandelwal is a Senior Research Associate at Jindal Global Law School (JGLS) and holds a Master of Laws (LL.M.) in Competition, Innovation and Trade Law from the London School of Economics (LSE). She is a graduate of the National Law Institute University, Bhopal.

I. PART I INTRODUCTION

A number of companies today provide their services for free to consumers. Social media networks, search engines, music streaming services, content sharing services etc. provide their services for free by using targeted advertising for revenues. This involves using large amounts of consumer's data which can be pay for these free services in the form of their data which is then transferred to advertisers and third parties. It has been seen that while consumers do want services with better privacy provisions, very few of them are willing to pay for such services. Digital players are not incentivized to come up with models which provide for data protection due to this 'privacy paradox'as consumers are not willing to shift to a different service provider which provides for better privacy provisions in exchange for a payment.

While the data protection law deals with the protection of personal data, however, this data can be acquired by the undertakings on the basis of consent, performance of a contract or legitimate interests.[1] The data protection law proves to be inadequate since undertakings can rely on these grounds which provide for lawful processing of data. Most of the times it is seen that even if consumers value their privacy, it is not possible for them to read the privacy policies of each and every website or platform that they use.

Even if they do, the terms of service do not give any control to the consumers to negotiate on how much of their data they are willing to give to these companies. Even under the consumer protection law, the consumers cannot lodge complaints against such digital giants as they are not made aware of the way that their data is being used. This limitation of the data protection law and consumer protection law is why we require the intervention of other laws in digital markets to protect privacy of consumers.

In numerous jurisdictions, there is a growing tendency by competition law authorities to intervene in the market to correct abusive practices by dominant

[1] General Data Protection Regulation (EU) (GDPR), art 6. The GDPR has been taken as model regulation of data protection law across jurisdictions since most data protection laws are based on GDPR.

undertakings. However, it is still debated whether competition law should be used to correct these practices. The research work argues that it should be. It has been seen that the digital undertakings gain dominance due to distinctive features of digital markets such as network effects which creates a 'winner takes all' situation. Because of having a huge market share, these dominant companies then abuse their position by gaining excessive consumer data and sharing it with advertisers and third parties. The harm to consumers due to large market share can be effectively corrected through competition law.

Intervention by competition law authorities is based on a consumer welfare standard i.e. the authorities intervene in a market only if they feel that non-intervention will cause consumer harm. Earlier, under the consumer welfare standard, the harm was restricted to high price ie to ensure that undertakings are not indulging in anti-competitive conducts which would increase prices for consumers. However, this is not the main concern of competition law in digital markets where services are provided for free in lieu of consumer's privacy. The article talks about this shift in the way that the consumer welfare standard is undergoing from price to privacy and what more can be done under this standard.

The article is divided into 5 parts: **Part II** of the article discusses the harms to consumers in digital markets due to network effects because of which platforms provide their services on zero prices. **Part III** then discusses how data protection law and consumer protection law are insufficient to deal with zero-price platforms. **Part IV** provides suggestions to improve the present consumer protection law framework to deal with the digital markets by bringing in the balance of regulation through data protection law, consumer law and competition law. **Part V** concludes the work.

II. PART II: POSSIBLE HARM TO CONSUMERS IN DIGITAL MARKETS

Since the digital platforms work on the revenue model of targeted advertising, companies provide their services on zero prices to enlarge their consumer base. This is because the digital markets have strong network effects.[2] Since most of the zero-priced platforms depend on advertising for their revenue, the success of the platform depends on the increased number of users. Larger consumer base makes the platform more lucrative for advertisers to advertise their

[2] Network effects occur when the value of the platform increases with the increase in the number of users on the platform.

products. Therefore, companies try to gain as much data as they can to use it for their own commercial advantage without the consumers knowing about it.

As per the Report of the Australian Competition and Consumer Commission (ACCC), Facebook stores activity information, such as photos and comments posted on Facebook and names and phone numbers of the user's contacts from the user's mobile device, even if the contacts are not user's Facebook friends. Facebook also links numerous ad interests to the user's profile and matches user to contact lists provided by advertisers. Similarly, it was seen that Google stores data from its products and services accessed in the past 7 years. Location data is collected by all these different products and services. Google also stores copies of photos without the consent of the user.[3]

These apps collect location data and store photos even if the location tracking settings and syncing of photos is turned off. The users have no control over the collection of their data. Users also have no control over the amount of advertisements that they have to see while using the platform. For instance, Facebook and Google policies clearly state that the user can only change the type of advertisements that it wishes to see but the number of advertisements would remain the same. Therefore, services are offered at an 'all or nothing' basis where consumers have no negotiating or bargaining power. Users are not allowed to opt out of any type of data collection or usage practices.

Due to network effects, it becomes easier forone undertaking to have a lot of data from its users which it can then use to its own advantage. An example of this can be seen in the case of *Google Shopping* case in EU where Google was giving more favorable positioning and display, in Google's general search results pages, of Google's own comparison-shopping service compared to competing comparison-shopping services.[4] This can be detrimental for other sellers and for consumers in form of less choice. Similar practice of search bias by Google can also be seen in the Indian context as well in the case of *Matrimony.com Ltd.* v *Google LLC*,[5] where its own specialized search services ranked higher than other vertical search services in the Search Engine Results Page. It gives Google the power to decide which businesses should succeed which creates entry barriers for new players trying to enter the market, thus stifling innovation.

---

3 ACCC, *Digital Platforms Inquiry* (Final Report, June 2019) (hereinafter 'ACCC Report').

4 Commission Decision of 27 June 2017, Google Search (Shopping), Case AT.39740.

5 2018 SCC OnLine CCI 1 <https://www.cci.gov.in/sites/default/files/07%20&%20%2030%20of%202012.pdf> accessed 27 June 2020.

Usually these entities are present in more than one market. For instance, Google develops mobile operating systems such as Android. In the case of *Google* Android in EU, Google required manufacturers to pre-install the Google Search app and browser app (Chrome), as a condition for licensing Google's app store (the Play Store).[6] All these services are also provided to consumers free of charge. This allows Google to accumulate data from all its services, thus, acquiring large amounts of data which then helps Google in providing more targeted advertisements.

As seen from cases such as *Google Shopping* and *Google Android*, consumers might suffer due to reduced choice and harm to privacy. Dominant undertakings such as Google do not give incentives to new players to enter the market. This can then result in lower quality due to lack of viable alternatives for consumers.[7] As seen from cases such as *Google Shopping* and *Matrimony* v *Google*, consumers are harmed as they no longer receive the most relevant results. This then leads to preference shaping through algorithmic manipulation by the dominant undertakings where the consumers are manipulated into buying a product or availing services of a website which is less suitable for them.

These undertakings also transfer the data to third parties without consumer's informed consent as seen from the *Facebook Cambridge Analytica* case where Facebook transferred user profiles to the data analytics firm Cambridge Analytica without consent. The Facebook's privacy policy says that while Facebook does not sell the personal data however, it has to 'work' with third parties to provide free services which means that the information with Facebook is still shared with third parties. While Facebook did get widespread negative press coverage which led to a 'Delete Facebook' campaign, it has been seen that only 1%-3% users deleted their account.[8] Users sticking to the same platform despite such a big scale harm to privacy is an indicator of lack of other alternatives.

---

6 'Antitrust: Commission Fines Google €4.34 Billion for Illegal Practices Regarding Android Mobile Devices to Strengthen Dominance of Google's Search Engine' (*europa.eu*, Press Release, 18 July 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581> accessed 27 June 2020.

7 For an analysis of how dominant undertakings harm the market by creating exclusionary effect, see Pankhudi Khandelwal, 'Interface between Competition Law and Data Protection Law in Monitoring Zero-Price Markets: Achieving the Balance of Regulation' (2020) 5 Indian Competition Law Review <http://iclr.in/wp-content/uploads/2020/05/INTERFACE-BETWEEN-COMPETITION-LAW-AND-DATA-PROTECTION-LAW-IN-MONITORING-ZERO-PRICE-MARKETS-ACHIEVING-THE-BALANCE-OF-REGULATION.pdf> accessed 27 June 2020.

8 Len Sherman, 'Why Facebook Will Never Change its Business Model' (*Forbes*, 16 April 2018) <https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model/#208a182464a7> accessed 20 March 2020.

III. PART III: INSUFFICIENCY OF DATA PROTECTION AND CONSUMER PROTECTION LAW

Data protection law can help in prohibiting the illegal transfer of data. However, most data protection laws around the world is based on the GDPR which allows the transfer of data on the basis of consent, performance of a contract or legitimate interests.[9] Accordingly, most of the platforms draft their data collection clauses broadly. For instance, Facebook states that it has to collect data to provide its services for free which qualifies it to collect data for the performance of a contract.

Usually, it is providedin the terms and conditions that if the consumers agree to use the services of the platform, they agree to the collection, usage and transfer of their data. These terms and conditions are long and not easily readable. Therefore, even if consumers are consenting to the privacy policies while using a platform, that consent is not informed or meaningful. Moreover, since the terms and conditions are provided on a 'take it or leave it' basis, the only option that the consumers have is to discontinue the use of the platforms if they are unhappy with the breach of their privacy. However, it is not possible for consumers to shift to any other platform due to network effects. For instance, users cannot use other platform except Facebook if all their friends are also on Facebook.

This leaves the consumers with no choice but to accept the terms and conditions. However, this does not mean that the consumers would not prefer an alternative which provides for better data protection provision. There is also an unequal bargaining position between consumers and giant techs which makes it more difficult for consumers to file cases against them. It is clear that companies such as Facebook and Google would not change their model as it would not be able to earn as much from consumers on subscription-based model as it can earn from advertisers through targeted advertising. Further, due to the distinctive features of online markets discussed above, it becomes difficult for other players to compete on a different model.

This situation can also not be corrected under the consumer protection law since, for consumer protection law to work; the consumers should be made aware of the way that their data is being used. Most companies do not share this information. For this reason, consumers do not feel the requirement to lodge complaints against these digital giants. This also brings in the problem

[9] GDPR (n 1).

of 'privacy paradox' where the consumers do not value their data or are willing to forego some of their data in exchange of these services.

One reason why consumers do not act to protect their privacy is they are not made aware about the costs of sharing their personal data. Therefore, it is argued that consumer's choice for privacy is not always expressed through their actions and the choices for consumers have to be formulated by regulatory bodies. For this purpose, along with data protection law and consumer protection law, the intervention of competition law is required to regulate these markets.

This can be seen in the case of Whatsapp/Facebook merger. After the acquisition of Whatsapp by Facebook, Whatsapp introduced new privacy policy which allowed for the sharing of information on Whatsapp to other Facebook family of companies. Whatsapp gave the option to the consumers to delete their Whatsapp account within 30 days if they do not want their data to be shared. Therefore, consumers were given an 'all or nothing' option where they had no bargaining power if they wanted to continue using the services of Whatsapp with better privacy provisions.

Numerous cases against this policy were filed across jurisdictions. The Italian Competition Authority fined Whatsapp under its consumer code for forcing the users to accept in full the new Terms of Use, and specifically the provision to share their personal data with Facebook, by inducing them to believe that without granting such consent they would not have been able to use the service anymore.[10]

Similarly, in Germany, the competition law authority formally initiated proceedings against Facebook and found that the social network was abusing its market power by violating data protection rules.[11] While this decision was stayed by the Higher Regional Court saying that violation of data protection rules does not fall within the jurisdiction of competition law, the Federal Court of Justice of Germany upheld the decision of the competition law authority stating that there were no serious doubts that Facebook was

[10] AGCM, 'WhatsApp Fined for 3 Million Euro for having Forced its Users to Share their Personal Data with Facebook' (Press Release, 12 May 2017) <https://en.agcm.it/en/media/press-releases/2017/5/alias-2380> accessed 16 March 2020.

[11] FCO, Case B6-22/16, *Case Summary, Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing* <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3> accessed 16 March 2020.

abusing its dominant position with the terms of use prohibited by the FCO.[12] The decision was based on the fact that the terms do not leave any choice for Facebook users.[13]

The difference between the Italian and German proceedings is that while the German authority had proceeded under competition law, the Italian authority fined Whatsapp under the consumer code. The decision of the Federal Court of Justice of Germany has given way for competition law authorities around the world to intervene in the conduct of dominant companies to ensure better privacy policies. One advantage of regulating through competition law is it provides for special responsibility on dominant companies to not abuse their position. Therefore, it puts more burden of compliance on larger companies than smaller companies thus making it easier for small companies to enter the market. More platforms in the market would provide more alternatives to the consumers. Further, more choice in the market would lead to companies competing on the basis of privacy protection.

In some countries, the competition law authority and the consumer protection body are the same. For instance, AGCM in Italy, FTC in USA and ACCC in Australia. The issues of competition law and consumer protection law are quite similar due to the consumer welfare standard under the competition law. Therefore, it is essential that where the regulatory bodies for the two areas of law are different, for instance, in India, both the authorities should work together to ensure protection of consumers from abusive or unfair practices leading to breach of consumer's privacy.

When the same practice by Whatsapp was challenged in India, in the case of *Shri Vinod Kumar* v *Whatsapp*,[14] the Competition Commission of India (CCI) held that data sharing from Whatsapp to Facebook is to improve the experience on Facebook. Users who do not want their data to be shared have the option to delete their Whatsapp account and therefore, it does not constitute an abusive practice. The CCI completely neglected the network effects of Whatsapp which makes it difficult for consumers to shift to any other platform even if they do not like the new privacy policy.

---

[12] 'Germany: Federal Court Summary Judgment: FCO Achieves Stage Victory against Facebook' (*DLA Piper*,25 June 2020)<https://blogs.dlapiper.com/privacymatters/germany-federal-court-summary-judgment-fco-achieves-stage-victory-against-facebook/> accessed 27 June 2020.

[13] *Ibid*. Since the decision of the Federal Court of Justice is in German, the translation of the decision by the above blog has been relied upon.

[14] Case No. 99 of 2016.

Further, CCI held that breach of privacy fell under the Information Technology Act and so it does not have the jurisdiction to decide violations under the same. This kind of decisions is precisely the reason why there is a requirement for competition law, consumer protection law and data protection law to work together in zero-price markets. The CCI, in such instances, should refer the issue relating to privacy to consumer court which can then decide whether the terms offered by Whatsapp are unfair to the consumers.

IV. PART IV: IMPROVED LEGAL FRAMEWORK FOR DIGITAL MARKETS

Most of the consumer protection law is modeled on protecting consumers from exploitation in monetary services. In the digital age, 'personal data' should be seen as equivalent to price or money that the consumer has to pay to avail services. This kind of change can be seen in EU in the Directive of the European Parliament on certain aspects concerning contracts for the supply of digital content and digital services.[15]

The Directive describes 'price' as money or a digital representation of value that is due in exchange for the supply of digital content or a digital service. It has been suggested that user data can also be viewed as an asset for digital platforms that can be sold, licensed, disclosed or exchanged with third parties[16] and thus using data more than required for the main activity of the platform should be deemed as an abusive or unfair trade practice under competition law and consumer protection law respectively as per the consumer welfare standard.

The data protection law should ensure that users are made aware of how and by whom their data is being used. For this purpose, we will need a stricter data protection law which does not allow companies to take more data than required through consent based on take it or leave it strategy. Further, the default settings on digital platforms should ask for consumers to 'opt in' rather than asking them to 'opt out'. Subscription based models such as those of Netflix; Amazon prime etc. should be promoted. Though such models might not be suitable for all kinds of consumers, however, there might be some consumers who might be willing to pay some amount of money for a platform with better privacy policies. It is essential that such consumers should

[15] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[16] ACCC Report (n 3).

be provided with alternative platforms where they do not have to worry about their data being misused.

Consumer protection law should be made stricter to provide consumers more bargaining power against digital giants. Further under competition law, authorities should be careful while assessing data – driven mergers. Merger regulation should include privacy as one of the considerations for competition. In the Facebook/WhatsApp merger case, while the European Commission stated that privacy and data security constitute key parameters of competition[17], it failed to assess the merger on the basis of harm to privacy. This omission by the Commission paved the way for WhatsApp to change its privacy policy to collect and share data with Facebook.[18] Therefore, while analyzing such mergers, it must be assessed whether the transaction would leave any incentives for digital players to compete based on privacy.[19] Further, as an ex post measure, companies should not be allowed to share data from one platform to another.

However, the authorities will have to be careful while regulating since some consumers actually prefer getting targeted advertisements and specialized services. Too much regulation might either lead to no incentives for the companies to innovate or if the platforms start charging high fees, it might prove to be too expensive for some consumers. Services such as social media and search engines have become essential in today's times and it is relevant that we do not create more problems than necessary for such platforms. It is, therefore, essential that such services are provided based on clear and informed consent and only the amount of data that is absolutely essential to provide these kinds of services is collected.

V. PART V CONCLUSION

Formulating the choice for consumers in digital markets should ensure both free services along with better privacy provisions. This would require stricter data protection rules and joint enforcement of consumer protection law with competition law. The laws presently are based on a non-interventionist approach. However, some regulation would be required to make sure that the

---

[17] *Facebook/WhatsApp* (Case No COMP/M.7217) Commission Decision C (2014) 7239 [2014].

[18] Case M.8228 - Facebook / Whatsapp, Merger Procedure Regulation (EC) 139/2004 (17 May 2017).

[19] Pankhudi Khandelwal, 'Interface between Competition Law and Data Protection Law in Monitoring Zero-Price Markets: Achieving the Balance of Regulation', (2020) 5 Indian Competition Law Review <http://iclr.in/wp-content/uploads/2020/05/INTERFACE-BETWEEN-COMPETITION-LAW-AND-DATA-PROTECTION-LAW-IN-MONITORING-ZERO-PRICE-MARKETS-ACHIEVING-THE-BALANCE-OF-REGULATION.pdf> accessed 27 June 2020.

consumers do not suffer harm due to their lack of awareness about the way that their data is being used.

Data protection law already provides for data minimization and purpose limitation i.e. data should only be collected for specified, explicit and legitimate purposes and should be relevant and limited to what is necessary to the purposes.[20] It should be monitored that these principles are followed under the privacy policies. Also, there should be a fixed time period for data retention. Further, privacy policies should give consumer the choice to negotiate whether they want extremely personalized services which requires access to unlimited data or personalization which is limited to the data that they have willingly provided. Collection of disproportionately large amounts of data should be considered an abusive practice. Further, the consumer welfare standard should be redefined to not just include price but also privacy and choice for consumers.

[20] GDPR (n 1) art 5(1).