



THE COLLECTION WITHOUT PERMISSION

Whatsapp's data sharing policy

By: Deeksha Bajpai

*From: New Law College
Bharati Vidyapeeth, Pune, Maharashtra*

ABSTRACT

In this research paper we will widely focus on the current perspective over the recent issue of the Whatsapp's data sharing policy with facebook. The recent acquisition of Whatsapp by Facebook has allowed Facebook to access Whatsapp's user data and user base. Whatsapp accounts for over 1 billion users who make over 500 million phone call, share 700 million photos, 100 million videos and 1 million messages a day. India with over 160 million active user is Whatsapp's biggest market and conceivably contributes significantly to above valuation. Whatsapp will become the owner of photos, text and information that Indians exchange on the app and if it decides, Whatsapp may share the personal information of its Indian users with Facebook. Other countries including European Union have taken initiative to prevent such kind of sharing of data. We will look into global as well as Indian perspective on the privacy issues with the help of Indian as well as international laws and talk about the encroachment of privacy by whatsapp's new data sharing policy to its parent company facebook.

This research paper covers two major research issues in this paper. Firstly, Whatsapp's data sharing policy is against Right to Privacy under Article 21. Secondly,

Whatsapp's free calling and messaging policy gives it a liberty to share the data with facebook.

Dealing with this question we will establish how data sharing policy of whatsapp with facebook is against right to privacy and personal liberty of a person. We are going to also establish that Supreme Courts argument that the free messaging and calling facility gives whatsapp liberty to share the data as users don't pay for the same, with the help of European Union's and other European country laws regarding data privacy. We will also show how major the effect of this encroachment of privacy by whatsapp over the Indian citizens.

• Introduction

In 21st century is it at all possible for us to argue that privacy is a fundamental right? Privacy is the subset of liberty. In this day and age only those political and moral orders that are given universal acceptance are human rights. Right to privacy comes under basic human rights given to each and every individual. If Right to privacy, Right to reputation or Right to Dignity is not at the core of the fundamental rights then no other right will be. Right to privacy comes under Right to life (Article 21). In Maneka Gandhi v. UOI case Supreme Court of India said that Art 19, Art 21, Art 14 cannot be read separately, they are the part and spirit of the constitution. Right to privacy is intrinsic to Right to dignity.

The recent acquisition of Whatsapp by Facebook has allowed Facebook to access Whatsapp's user data and user base.



Whatsapp accounts for over 1 billion users who make over 500 million phone call ,share 700 million photos , 100 million videos and 1 million messages a day. India with over 160 million active user in Whatsapp's biggest market and conceivably contributed significantly to above valuation. Whatsapp will become the owner of photos , text and information that Indians exchange on the app and if it decides , Whatsapp may share the personal information of its Indian users with Facebook. Other countries including European Union have taken initiative to prevent such kind of sharing of data.

- **Research Question**

1. Is Whatsapp's data sharing policy against Right to Privacy under Article 21 ?
2. Does Whatsapp's free calling and messaging policy gives it a liberty to share the data with facebook ?

- **Hypothesis**

In this research paper I want to throw some light over the issue that whatsapp's new data sharing policy is against article 19 and article 21 of the Indian constitution.I will also draw a comparative study between the privacy laws in and around the world.

- **Research Methodology**

This research paper is based on doctrinal research. It talks about the current case of whatsapp sharing its data withfacebook. The research will be based on direct criticism and the suggestive measures to be taken by the government.

- **Scope of Research**

In this research paper , we shall be primarily be focusing upon international laws on privacy and laws in India Constitution along with the general perspective on the current issue in nationally as well as internationally. It Act will also come in the picture.

- **Significance**

Through this research I want to draw the attention towards understanding the basic nature of data privacy in the modern digital economy. This research paper is crucial to interpret article 19 , article 21 which are at stake.

CHAPTER 1- WHATAPP'S DATA SHARING POLICY V/S RIGHT TO PRIVACY

Facebook paid \$22 billion (Rs.1,472.79 crore) – or, just about 2.5 times Facebook's 2013 gross incomes – to purchase WhatsApp, an organization with net loss of over \$38 million at the time. Why? One clear reason, obviously, was to fight off potential rivalry and begin its way towards turning into an online networking combination.

WhatsApp accounts for over 1 billion users who make over 500 million phone calls, share 700 million photos, 100 million videos and 1 billion messages a day.India, with over 160 million active users, is WhatsApp's biggest market and conceivably contributed significantly to the above valuation.

WhatsApp may turn into the owner of the photographs, writings and data that Indians trade on the application, and in the event



that it chooses, WhatsApp would have shared the individual data of its Indian clients with Facebook, outsiders or scamsters.

Supreme Court in its latest decision upheld that-

Right to privacy as a fundamental right and extending it to include informational privacy, may impact the collection and sharing of data by technology giants such as Google, Facebook, Apple and WhatsApp in India. This decision arms natives with the privilege to address or question how famous websites and apps utilize and share user data.

The nine-judge bench in its decision talked about the issue in detail and perceived use security as a part of the right to privacy. It highlighted the threats of sharing data utilizing the different technology means available to us.

The judgment gives individuals the privilege to specifically approach the court if their right to privacy is under danger. It could give legal backing to petitions in courts on how popular social networking sites and administrations are handling, saving and sharing user data.

Recognizing the importance of informational privacy, Chief Justice J.S. Khehar and Justices D.Y. Chandrachud, R.K. Agrawal, S. Abdul Nazeer said, "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well."

CHAPTER 2- RIGHT TO PRIVACY UNDER RIGHT TO LIFE

In spite of the fact that no particular reference in the Constitution, the right to privacy is viewed as a 'penumbral right' under the Constitution, i.e. a right that has been proclaimed by the Supreme Court as basic to the right to life and freedom. Right to Privacy has been culled by Supreme Court from Art. 21 and a few different arrangements of the constitution read with the Directive Principles of State Policy. Although no single statute gives a crosscutting right to privacy; different statutes contain arrangements that either verifiably or unequivocally protect this right. For the first time in **Kharak Singh v. State of U.P**¹ question whether the right to privacy could be implied from the existing fundamental rights such as Art. 21 came before the court, it was held that –

*Although the majority found that the Constitution contained no explicit guarantee of a "right to privacy", it read the right to personal liberty expansively to include a right to dignity. It held that "an unauthorized intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common law right of a man -an ultimate essential of ordered liberty, if not of the very concept of civilization"*²

¹AIR 1963 SC 1295

²https://www.lawctopus.com/academike/article-21-of-the-constitution-of-india-right-to-life-and-personal-liberty/#_ednref71



In the case PUC v. Union of India³ Supreme Court held that

We have; therefore, no hesitation in holding that right to privacy is a part of the right to “life” and “personal liberty” enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy; Article 21 is attracted. The said right cannot be curtailed “except according to procedure established by law”.

In the latest Supreme Court judgment recognizing the importance of informational privacy, Chief Justice J.S. Khehar and Justices D.Y. Chandrachud, R.K. Agrawal, S. Abdul Nazeer said, “Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well.”

**CHAPTER 3
NO WAY TO OPT OUT**

4

WHATSAPP’S NEW PRIVACY POLICY

WhatsApp can now share data, including your phone number, with Facebook, letting it better target adverts and improve friend suggestions.

Facebook and WhatsApp will be able to link accounts using technology that detects when a phone has both apps installed

It will also gain data such as device type and software information, although messages will continue to be encrypted

The privacy policy also allows business accounts for the first time. WhatsApp plans to make the app a home for customer service, allowing companies to contact users

The new policy also reflects recent changes to WhatsApp such as voice calls and its web version. Users can opt out of sharing data with Facebook, but will have to agree to the privacy policy within 30 days. Later in 2016, WhatsApp stopped some data sharing in Europe after a privacy backlash

Another catch is that even if you opt out of the data-sharing, WhatsApp will share some of your data with Facebook for product improvement, usage behaviour, fighting spam, abuse, or infringement activities.

**CHAPTER 4-
FREE SERVICE OBJECTION BY
SUPREME COURT**

The court's greatest objection to decision that WhatsApp violated individual's privacy was that individuals did not "pay" for the service as they would for a customary telecom benefit. internet commerce has however overturned traditional business model. In the web age, buyers help WhatsApp (and numerous other web based organizations) procure from income streams, regardless of the possibility that user don't give a physical check specifically to WhatsApp.

In this case, Facebook paid WhatsApp more than 20 times its annual revenue even though WhatsApp was actually making loss. So, the question that consumers did not pay WhatsApp directly is not required to determine whether or not WhatsApp is profiting from the users, which it clearly is.

For example, in the physical world, I made a street over "poromboke" or open land, and many individuals utilize the street thus it turns into a highway. On that premise, would i be able to guarantee I now claim the highway? Will the court say, since individuals did not pay to clear the street, the street is presently mine?

By a similar logic, WhatsApp had already accepted more than sufficient remuneration from Facebook (and possibly, the market).



Thus there is no support or legal basis required by the Supreme Court to prioritize WhatsApp's claim over the person who created the texts and content and have rights to transfer information to WhatsApp.

CHAPTER 5- EUROPIAN UNION’S VIEWPOINT OVER DATA TRANSFER

European Union privacy chiefs said Facebook must stop processing user data from its WhatsApp messaging service while they are still investigating the new privacy policy changes related to the data collection of users .

The Article 29 Working Party, made up of privacy chiefs from across the 28-nation EU, said that for Facebook it had genuine worries about the sharing of WhatsApp clients' information for purposes that were not included in the terms of service and privacy policy when existing users joined Whatsapp.

The group is not the first one in Europe to condemn WhatsApp's new data sharing policy. Regulators in Germany also ordered Facebook to stop collecting WhatsApp users' data and delete any information already transferred.

European privacy protection watchdogs don't shy away from focusing on enormous US technological firms, as prior investigation concerning Facebook, Alphabet's Google or Microsoft have appeared. Just their fining powers still needs teeth, which will change under new EU decides that will produce results over the coalition in 2018 with punishments

conceivable of as much as 4 percent of an organization's worldwide yearly deals.

The EFF noted that unlike some other tech companies, "WhatsApp does not explicitly state that it prohibits third-party access to its user data, nor does it say that third parties are prohibited from allowing WhatsApp user data to be used for surveillance purposes".⁵ Elizabeth Denham, the Information Commissioner of UK said that if Facebook is found to share data without any proper consent, it may “face enforcement action from my office”. The ICO has the power to fine companies up to £500,000 for the breach of Data Protection Act.

German regulators had earlier banned WhatsApp's data sharing over its privacy issues. European countries are stringent regarding protection of its user data. The EU is also pondering over an E-Privacy Directive to protect its citizens and imposing regulations on internet communications companies similar to traditional telecom companies.

CHAPTER 6- TRADITIONAL PRIVACY ARGUMENT WON'T WORK

If the WhatsApp issue is tarred by the Aadhaar brush, Chief Justice Khehar is unlikely to pass an order in favor of the petitioners, who have asked for a ruling preventing WhatsApp from merging the data with Facebook. In multiple orders from

⁵<http://www.telegraph.co.uk/technology/2017/07/11/whatsapp-not-enough-defend-users-against-governments/>



2010-2015, the Supreme Court repeatedly held it was not striking down Aadhaar as unconstitutional [based on the government assurance that participation in the program was voluntary](#) (and not mandatory). But Chief Justice Khehar has markedly departed from this position. On February 7, Chief Justice Khehar (along with Justice N. V. Ramana) tacitly approved the idea of linking all mobile phones (via the sim cards) to the owners' Aadhaar cards in the interest of national security (because it was feared unverified mobile numbers could be used for terrorist and criminal activity).

This even though Attorney General Mukul Rohatgi had pointed out how vital mobile payments were to citizens in the aftermath of demonetisation. The Supreme Court's change in position from asking that participation in Aadhaar be voluntary to implicitly allowing the government to implement mandatory participation clearly demonstrates that the present chief justice places more importance on national security arguments rather than privacy objections. Chief Justice Khehar and Justice Chandrachud have already alluded to their doubt that users can scarcely demand free speech rights in a "free" service that they do not pay for. If the issue is with regard to privacy, the constitutional bench in the Aadhaar case is already considering whether there is a the right to privacy in the Indian constitution. On the whole, the court has not found the right to privacy objection persuasive in the Aadhaar context⁶

⁶<https://thewire.in/120714/chief-justice-khehar-shouldnt-allow-whatsapp-share-indian-user-data-facebook/>

CHAPTER 7-

THE BIG BLOW TO INDIAN USERS

India, has over 160 million [active users](#), and is WhatsApp's biggest market and conceivably contributed significantly to the above valuation. Other countries have taken initiatives to prevent the data sharing policy of WhatsApp. In the European Union, data regulators have [already warned](#) WhatsApp about their data sharing policy of European citizens with Facebook, with the social network firm [agreeing](#) last November to temporarily stop sharing data.

Contrary to European Union, India has made no move to prevent Facebook and WhatsApp from mixing their user information databases. Chief Justice Khehar and Justice Chandrachud nearly declined to admit public interest litigation on this matter in January. The court said that users can opt-out and expressed doubts on whether users can claim a right to privacy or free speech in a "free" communication program like WhatsApp messenger.

It may be important to point to the court that if it fails to intervene in the matter, WhatsApp will have access to and have the right to share only Indians data whereas user data of other countries will belong to its citizens only and WhatsApp and Facebook will not be able to merge and/or sell the information of European citizens. The data of India's citizens – texts, photos, usage data, names and mobile numbers of all contacts in their address book (irrespective of whether those people use and consented to WhatsApp's policies) would not be protected.



Today India is among the fastest growing economies but a sizable portion of its population continues to struggle to earn enough to pay for basic needs, medical costs and education. Judges too are mainly focused upon cases deciding people's access to basic necessities of life and in this context, worries about privacy and personal information often seems out of touch. Insisting the court intervene in the WhatsApp case based upon fears of potential privacy violation is therefore an uphill battle and an unnecessary one by failing to intervene, the Supreme Court will be helping the corporations to claim property rights in Indian citizens data and information in a way they cannot do with any other country's citizen's data and information.

Thus, when other countries are so assiduously and ardently protecting its citizen's data, if the Supreme Court looks the other way and allows Indians' data alone to deal with the private social media companies, the court will be doing a disservice to its people.

CHAPTER 8- INTERNATIONAL PRIVACY POLICY V/S INDIAN PRIVACY POLICY

No separate laws like EU-

Unlike the European Union, India does not have any separate law which is designed exclusively for the data protection. However, the courts on several occasions have interpreted "data protection" within the ambits of "Right to Privacy" as implicit in Article 19 and 21 of the Constitution of India.

Europe has been on the forefront of privacy legislation and recently the EU came out with draft 'Digital Single Market' plan that has a default 'opt-out' for data sharing by users, instead of a default 'opt-in' as is the case today. Similarly, Indian users should be given the option to opt out of specific features instead of a singular 'I Agree' button.

Information Technology Act-

The strongest legal protection provided to personal information in India is through section 43A of the Information Technology Act and the Information Technology Rules, 2011 developed under this section.

The provision requires a body corporate who 'receives, possesses, stores, deals, or handles' any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which they are held liable to compensate those affected.

Penalty⁷-

Any corporates who fail to observe data protection norms may be liable to pay compensation if they are negligent in implementing and maintaining reasonable security practices and thereby cause wrongful loss or wrongful gain to any person.

Body corporates may be exposed to criminal liability under Section 72A of the IT Act if they disclose personal information with the intent of causing wrongful loss or obtaining a wrongful gain. This Act includes the disclosure of personal information given in

⁷<http://www.news18.com/news/india/right-to-privacy-data-protection-laws-in-india-1500047.html>



confidence as an unfair trade practice (as defined under section 2 (r)) and includes mental or emotional harm resulting from damage to property, among other things, as a harm.

CONCLUSION-

In October 2015 we saw a billion mobile phone users, with an active base of 902 million. Among these, there are about 300 million smart phone users that utilize their phones for tasks such as shopping, calling cabs, ordering food as well as taking online diploma courses and making payments for various items.

It then becomes clear that the ‘product’ is not the app but the data that the user is generating while using the app. using complex algorithms, the patterns and preferences of the user are identified. The primary use of this processed data is for targeted advertisements. However, the user has little or no knowledge of what happens; to this data beyond advertisements. It may be sold to the highest bidder for use in development of other apps or it may even be shared with law enforcement agencies for threat-profiling.

It’s not just the matter of what can be done with the collected data, but also about what kind of data is collected, how much of it is collected, for how long it can be held, and who owns the data. The application owners have incentives here, so, it’s in their best interest to get as much information as they can. The incentives come from the potential of data, which drives innovation in the market.

Recently, the Supreme Court issued notices to WhatsApp over an appeal against the instant messaging service for not ensuring the privacy of its users and to the Centre for seeking regulations to protect personal information. This response of our courts is in stark difference with that of Germany’s Commissioner for Data Protection and Freedom of Information, who ordered Facebook to cease collecting information of German WhatsApp users and asked it to delete all data that has been shared previously. It went on to state that Facebook and WhatsApp should act as independent companies and process user’s data on separate terms and conditions. If we were to highlight main difference in the way the same issue was tackled by two different institutions, then it is clear that the order of the German authority is primarily focused on the entity that will be collecting the data, in this case, Facebook and protects the end user’s interests. On the other hand, the last option for an Indian user who does not wish to share his personal information is to not use WhatsApp’s service.

It is this differentiating treatment towards the same solution that warrants a close look at the data privacy laws in our country. In their present form, provisions in the Information Technology Act (2000) and subsequent amendments that try to address privacy concerns are piecemeal in nature. We cannot apply the principles of ‘notice’ and ‘consent’ in an era where smart devices are monitoring heart beats. In the current data collection practices consent system is broken, and pointless. Legal jargon often entangles and confuses users. There is a dire need for new privacy policy in the modern



digital era . Privacy laws will only work better if we clearly differential who they will regulate and what they will protect.

BIBLIOGRAPHY-

1. <https://www.theverge.com/2016/8/25/12638698/whatsapp-to-start-sharing-user-data-with-facebook>
2. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-facebook-user-data-share-summer-app-privacy-eu-a7679971.html>
3. <http://www.telegraph.co.uk/technology/2017/07/11/whatsapp-not-enough-defend-users-against-governments/>
4. <https://thewire.in/120714/chief-justice-khehar-shouldnt-allow-whatsapp-share-indian-user-data-facebook/>

Literature review

BOOKS

1. **The constitution of India (Bareact).**
2. **MP Jain , (right to life article 21)**

WEBSITES

5. <https://www.theverge.com/2016/8/25/12638698/whatsapp-to-start-sharing-user-data-with-facebook>
6. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-facebook-user-data-share-summer-app-privacy-eu-a7679971.html>
7. <http://www.telegraph.co.uk/technology/2017/07/11/whatsapp-not-enough-defend-users-against-governments/>
8. <https://thewire.in/120714/chief-justice-khehar-shouldnt-allow-whatsapp-share-indian-user-data-facebook/>
