Ayana Legal

THE BUZZ

Monthly Newsletter By Team Ayana Legal

Data Collected By WhatsApp

The new privacy policy makes a distinctions between - data that is provided by the users and the data that the platform automatically collects.

a) Data Provided By User

The data provided for by the user includes details of their phone number, their name; media that is forwarded, connections or contacts using the platform, any transactions made on the platform and the user's profile status.

b) Automatically Collected Data

The automatically collected information includes an users usage, activity and logs on the platform, information of the device the platform is being used on (IP address, the hardware model of the device, signal strength, battery level, browser information etc.)

WhatsApp's New Privacy Policy

All the great ages were defined by cataclysmic events, American Revolution (1765–1783), The Circassian Revolution of 1970, The French Revolution of 1780's. The Digital age was forever revolutionized in the year of 2009, the birth of WhatsApp. The existence of the WhatsApp messaging the official first release of WhatsApp launched in November 2009, exclusively at the App Store for iPhone. In January 2010, support for BlackBerry smartphones was added; and subsequently for Symbian OS in May 2010, and for Android OS in August 2010. Gone were the days of messaging through Yahoo messenger and MSN messenger, and anxiously waiting for a reply. WhatsApp took over the market in one fell swoop and has never looked back and now after nearly 11 years WhatsApp has come with its biggest change yet.

In January 2021, social media platform WhatsApp released it's new privacy policy affecting non European users. The new privacy policy clearly states that there is certain data that the platform has to necessarily collect if it has to operate and make available to the user certain features (e.g. giving your mobile number to create

Why Non-European Users Only?

The reason behind why only Non-European Users of the platform are affected by the new privacy policy is because of the presence of the GDPR in the EU.

GDPR - General Data Protection Regulation is the law on data protection and privacy in the EU and came into effect in 2018.

The GDPR was introduced with the view of allowing individual users to have more control over their data. The consumers are given the option to opt in or opt out of sharing their data. It also puts an obligation upon organizations collecting and maintaining personal data to not misuse, the breach of which is punishable.

The Personal Data Protection Bill, 2019

The bill was introduced in the parliament in 2019 and is yet to come into force.

The Bill aims to govern the processing of personal data and sets of rights of individual users/ citizens and obligations over data fiduciaries and social media intermediaries. The Bill also aims to create Data Protection Authorities.

an account).

The privacy policy seems to stress on the fact that WhatsApp is a part of the Facebook company stating that WhatsApp can receive information regarding users from the other services provided by Facebook company. Not only does WhatsApp receive information but, the privacy policy also discusses how WhatsApp may share such user information to other Facebook Company products - which is to aid in the creation of more personalized content and features.

The Puttaswamy Judgement

Through the Puttaswamy judgement (**K.S. Puttaswamy And Anr. v. Union of India And Ors.**) the apex court has held that right to privacy is indeed a fundamental right.

The judgement defines informational privacy as the right of an individual or "*an interest in preventing information about the self from being disseminated, and controlling the extent of access to information.*" Emphasizing that informational privacy is a right the state ought to protect, the court has given a 3 element test defining the extent to which individual privacy should be protected -

• "There must be a law that justifies breach of privacy

• The scope and nature of the law imposing restrictions must be reasonable

• The means which are adopted restricting privacy must be proportional to the objective sought to be fulfilled by the law."

Indian Laws On Privacy

Currently, India's privacy and data protection laws are limited to the Information Technology Act of 2000. Section 66E of the Act while defining the punishment for violation to privacy limits the meaning of the term 'privacy' to 'image of private area of a person'. Section 72A of the Act, intentional disclosure of information without the consent of the person concerned and in breach of the lawful contract has been also made punishable.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provides that any body corporate that collects and stores

A penny for your thoughts?

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."

- David Brin

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

- Edward Snowden

"The right to be left alone is indeed the beginning of all freedom"

- William O. Douglas

[Public Utilities Commission v. Pollak, 343 U.S. 451, 467 (1952) (dissenting)]

Thank You

Team Ayana Legal thanks you for the trust. Till we are back with our next edition, stay safe and keep smiling.

sensitive personal data should provide a privacy policy to it's users. Such data can only be collected with user consent in writing. The collection of the data too can only be for a lawful purposes with the option withdraw their consent from such collection of data. The rules also stipulate that data may not be disclosed with third parties unless there is an explicit contract with the consent of the user.

The Step Ahead

The fear in the wake of the new Whatsapp privacy policy serves as a much needed wake up call towards the deficiency of data and privacy protection laws and safeguards in our country. It is of much importance and high time that we developed comprehensive data protection laws to secure individual privacy and prevent such scares of data violation in the future. The Union government constituted Group of Experts on privacy has proposed nine privacy principles for securing user data and information privacy that are to serve as guiding principles for future laws. They are:

(i) Notice to be provided before personal data is collected

(ii) Choice and consent to provide information

(iii) Data collection limitation only for purposes in notice.

(iv) Destroying or removal of such data from data bases after purpose is achieved.

(v) Access to data and allowing of correction to data provided to be allowed to users.

(vi) Data collected shall not be disclosed to third parties, made public or published, unless consent is received.

(vii) The data should be secured through reasonable security safeguards.

(viii) The security system must be proportional the extent and sensitivity of the data collected.

(ix) The information collecting body shall be held accountable and must include mechanisms to implement privacy policies.