iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** X **Month of publication:** October 2021

DOI: https://doi.org/10.22214/ijraset.2021.38618

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue X Oct 2021- Available at www.ijraset.com

Personal Data Protection: Rules among exceptions and WhatsApp

Pushpesh Paliwal
Nalsar, India

I. INTRODUCTION

The increasing amount of data generated by devices we interact with requires the data to be protected more zealously. The Personal Data Protection Bill, 2019 seeks to bring in a data protection regime to curb and prevent misuse of personal data. In this respect, it is pertinent to examine a class of data which has been unregulated or escapes the regulation – metadata. Metadata is data about data. It is a structured information which describes the source of information. The source can be an image, a report, database, etc. The processing is done of the information about the data rather than the data itself. The metadata can be resolved into smaller parts. This is called the granularity of metadata. Thus, granularity refers to the individual objects in the dataset or collection. The granularity levels of metadata are not completely separate from each other but processors may choose to focus on certain levels. Apart from granularity, there are different levels of metadata –

1) *Metadata for Discovery:* The minimum amount of data that can convey the nature and content of resources available. It includes data such as where the data is, who holds the data or what are the resources that exist.
2) *Metadata for Evaluation:* It adds a level of detail to the data, providing information as to its categorisation and allows the user to decide if the data is something which the user wants to access.
3) *Metadata for use:* The details of use of the resource, access to user, and other such information is provided.

It is important to understand and regulate metadata because it can be used for profiling users. The anonymous profile can contain data as valuable as personal information. In 2012, the FBI was able to track down a wanted hacker using the location metadata attached to an image of his in a blog. Therefore, the anonymous metadata can still be used for profiling the users. The paper will focus on the terms and conditions of service of WhatsApp. The metadata which is collected by WhatsApp and the Terms of Service are not in compliance with the Personal Data Protection Bill. The Terms of Service of WhatsApp are analysed in reference to the Personal Data Protection Bill.

II. STANDARDS GOVERNING METADATA

The European Committee on Standardisation (CEN) published a pre-standard on metadata of Geographical Indicators. The standards were assimilated by International Standardisation Organisation's Technical Committee 211. It culminated in the ISO 19115:2003 Geographic Information Metadata. The following provisions are made by the standards-

The appropriate information should be provided to the data producers so that they can characterize the geographic data

1) Organisation of the metadata and its management is to be provided for
2) Base characteristics to be given so that users can apply the geographic data efficiently
3) The reuse, retrieval and discovery of data is to be provided for
4) The users should be able to ascertain if the data in a certain block is of their use

These standards were adopted by the Open Geographical Consortium (OGC). Subsequently, all the European national bodies have adopted the standard. The ISO 15836 or Dublin Core Metadata elements set is a popular standard for other types of metadata such as e-Government. An effort towards metadata standards it the INSPIRE directive of the European Union. It focuses on developing rules for implementation to be developed in accordance with global standards.

The following are the INSPIRE requirements –

a) Spatial data sets to conform to harmonization rules of implementation
b) Use and access of spatial data sets and services to be conditional
c) The validity of data sets and their quality is to be maintained
d) The management, maintenance, distribution and establishment of data sets is to be controlled by public authorities
e) Public access to be limited and the reasons for the same are to be known

The European Union directives also mandate that the metadata should be searchable and its contents can be viewed. These standards are optional requirements which can be voluntary adopted by the organisations.[1]

III. THE IT ACT AND SPD RULES FRAMEWORK

The framework for protection of personal data is based on the Information Technology Act, 2000. The Act[2] under Section 87 provides for the government, the power to make rules. The sub section 2 (ob) binds the government to make rules as to the reasonable security practices and the sensitive personal information or data under Section 43 A. The Section 43A is titled compensation for failure to protect data. It prescribes damages to be paid by the body corporate which causes wrongful loss to any person by reason of not maintaining reasonable security practices or failing to implement them. The explanation to the section defines sensitive personal information or data. The sensitive personal data is the personal information which the Central government, after consultation with associations or professional bodies, declares to be so. Thus, it is the duty and power of central government to notify what sensitive personal information is and make rules with respect to its use. The rules have been framed by the government as The Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules, 2011. The rules define what data or information is, how it is to be processed and stored while outlining the contours of personal data. The definition of data is referenced back to the Information Technology Act. Section 2 (1) (o) defines data. Data is a representation of facts, knowledge, information, instruction or concepts which are to be processed, or are being processed or have been processed in a computer network or computer system and are prepared in a formalised manner or are being prepared in such a manner. These may be internally stored in the computer's memory or stored in a storage device in any form. Similarly, Section 2 (1) (v) provides an inclusive definition for information. Information includes databases, codes, sound, voice, computer programs, images, data, message, text, micro film and computer-generated microfiche. The information is further categorised into personal information and sensitive personal information or data. Rule 2 (1) (i) defines personal information as any information which can directly or indirectly relate to a natural person. This includes information which is available with a body corporate or that is likely to be available and is capable of identifying the person.

The sensitive personal data has been defined under Rule 3 in consonance with Section 43A of the IT Act. The following data has been declared to be sensitive personal information under the rule – biometric information, information on medical records and medical history, sexual orientation, physiological, mental and physical health conditions, the details of payment instruments such as credit card, debit card, etc. and financial information including bank accounts, the details which relate to these categories of information, provided to a body corporate to avail any service. It also includes any information which is provided, stored, or received for processing by a body corporate, under a contract or not but is covered by the provision. The information which is available in the public domain is exempted. The exception also provides that any data or information which is accessed through the Right to Information Act, 2005 or any other law which is in force will not be considered as sensitive personal data or information. Thus, defining the contours of what data or information is considered to be sensitive.

The ensuing rules provide how the data is to be protected. Rule 4 mandates a body corporate receiving, storing or handling the information to publish a privacy policy on its website. It must also ensure that the provider of the information can view the privacy policy. The provision is applicable when the information collected is personal information including sensitive personal data or information. The requirements are for the privacy policy to be clear, with easily comprehensible statements. It should provide the type of personal or sensitive personal information which is to be collected, its purpose and use and the security procedures and practices in place. The privacy policy should also allow the disclosure of the data collected to the user. The rule 5 states the conditions under which a body corporate can collet data, including personal and sensitive personal information. The consent of the user is an important pre-condition for data collection. The rule 6 and rule 8 relate to such data collection and disclosure and the attendant practices and procedures. These rules govern the personal and sensitive personal data protection in the present framework.

The constitutional provision which is highlighted in the discussions around privacy is Article 21. The Article 21 provides a right to life which imports the idea of privacy. In the KS Puttaswamy case,[3] a nine-judge bench of the Supreme Court was constituted to determine if privacy is a constitutionally protected right. The Court analysed the precedents regarding the right to privacy. The

[1] CRAGLIA, M., KANELLOPOULOS, I. AND SMITS, P., 2007, MAY. METADATA: WHERE WE ARE NOW, AND WHERE WE SHOULD BE GOING. IN *PROCEEDINGS OF 10TH AGILE INTERNATIONAL CONFERENCE ON GEOGRAPHIC INFORMATION SCIENCE*.

[2] THE INFORMATION TECHNOLOGY ACT, 2000, NO. 21, ACTS OF PARLIAMENT, 2000(INDIA)

[3] AIR 2017 SC 4161

Court holds that the Canara Bank judgement affirms that the right to privacy emerges from the Article 19 guarantee of liberties and the protection of personal liberty and life under Article 21. The ensuing cases of Kharak Singh and Gobind have consolidated this stance. The commitment of India to the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR) enables further support to such an interpretation. The Court observed that metadata and its abilities are yet to be perceived fully. Citing Christina Moniodis, the metadata is capable of creating new knowledge about the individual, information which the individual is also not aware that it possesses. In the present age, there is a systematic monitoring of the individual and the data which is generated by them. The metadata consists of data sets which are capable of being searched, can have linkages with other data and have scope of being permanent. The challenges to security which arise from such collection of metadata are both from non-state as well as state actors. Yvonne McDermott states that the rise of the quantified self through constant monitoring of oneself using devices such as trackers, social networking data, etc. may result in data being collected about the individual as well as the people around them. A consent-based model for data collection is inadequate because the data can also be repurposed for other applications. The protection of such data, especially metadata, is necessary also from a social perspective. It must be ensured that the collection of data does not allow for profiling, violating the principle of non-discrimination on the basis of race, ethnicity, etc. The protection is also needed from the state so that the state collects data only for legitimate purposes. The data collected as such should not be used unauthorized and for purpose other than the one stated. The Court acknowledged the importance of digital technology but emphasised on the protection of data generated through such technology.

IV. THE PERSONAL DATA PROTECTION BILL AND THE NEW FRAMEWORK

The Personal Data Protection Bill[4] seeks to replace the framework of the present rules with an updated standard to global data protection practices. The applicability of the Act presents an interesting approach. The Section 2 (B) of the Act excludes the applicability of the Act from the processing of anonymised data. The only exception is Section 91 which exempts the governments processing of such data. A number of such exceptions are present in the Bill. Section 3 (28) of the Bill defines personal data. The personal data is data which relates to a natural person and covers data which may be directly or indirectly used to identify such a person. The data may be online or offline and includes data from which inferences can be drawn for profiling of the user. The definition is an expansive one and would include most of the metadata which is identifiable as personal data. The protection to such data is also provided for in the Bill. But it is the exceptions which are cause of concern. The data collection framework is based on consent to be provided under Section 11. The exceptions to such a requirement of explicit consent are Section 12,13, and 14. Section 14 provides the conditions, subject to which and the regulations framed that a mandatory consent can be waived off. The reasonable purposes for which such a consent can be waived includes network and information security, detection and prevention of fraud. Section 15 provides for the Central Government to notify the categories of data as sensitive personal data. The sub clause (2) provides that the authority can notify such safeguards or restrictions on continuous, systematic or repeated collection of data. The bill provides a right to be forgotten, correction and erasure of data. The bill is an update over the present rules and is in consonance with international standards.

V. WHATSAPP AND THE DATA COLLECTED

The metadata regulations are operative in the usage of digital technologies, especially applications such as messengers. WhatsApp Messenger is a popular mobile messaging app. The privacy policy published by it provides the data collected, procedure for seeking the data collected, etc. The present rules of the framework do not have any explicit provisions which prohibit collection of metadata and its processing. The following data is collected by WhatsApp without explicit consent of the user – device information such as hardware id, battery level, etc., log files, time spent on the app, signal strength, mobile network provider information, tokens associated with Facebook products, approximate location based on the IP address of the user, etc. The data is collected using anonymous tokens but a majority of it can be used to profile the user. The network information, battery level, hardware id, location information can be used for profiling of the user.[5] The anonymisation of data implies that it can be exempted under Section 2(B) of the Bill. Further, Section 14 of the Bill provides the exception of waiver of consent for purposes of information security. The collection of the information about network is provided for network and information security. The purpose is classified as reasonable under the Bill, thus nullifying any protection. The Bill as a whole is built up on a number of exceptions. The data collection by body corporates under the Bill can be exempted through a number of provisions.

[4] THE PERSONAL DATA PROTECTION BILL, 2019, BILL NO. 373, LOK SABHA, 2019(INDIA)

[5] WHATSAPP.COM. 2021. *PRIVACY POLICY*. [ONLINE] AVAILABLE AT: <HTTPS://WWW.WHATSAPP.COM/LEGAL/UPDATES/PRIVACY-POLICY> [ACCESSED 11 MAY 2021].

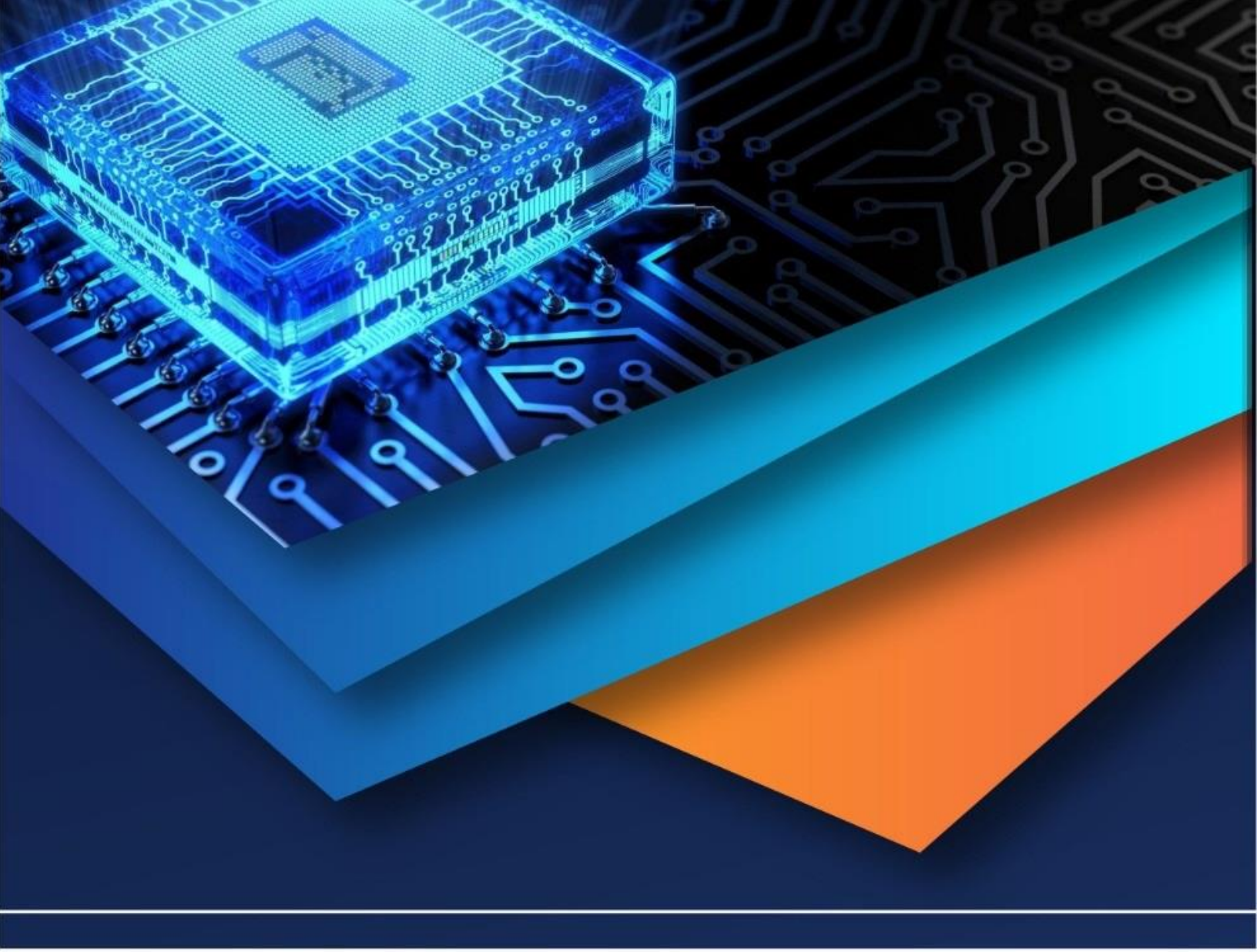
The framework provides hollow protection to personal data. The classification of data as sensitive by the government provides no additional protection to such data from exemptions. The data policy of WhatsApp is perfectly capable of flying under the radar through the exceptions provided in the Bill.

VI. CONCLUSION

The growth in digital technology and use of such devices has led to a disproportionate increase in the amount of data which is generated. The data which is generated consists of two categories – the explicit data which is created and the metadata, data about data, which is generated automatically, every time some data is generated. The regulation of metadata has been a concern of a number of frameworks. The INSPIRE framework is the latest metadata framework which governs the collection, use and regulation of metadata. The frameworks are optional in nature and can be implemented by organisations who volunteer to abide by such frameworks. The optional nature of these framework makes the protection provided by them to be very weak. The present framework of data protection consists of the Information Technology Act and the Sensitive Personal Data Rules. The Act places the power to make rules with the Central Government. The Central Government has to notify the categories of data which are to be classified as personal data and sensitive personal data. The government has notified the rules titled The Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules, 2011. The rules provide for the security measures which are to be adopted when protecting the personal data which is collected from the users. It provides a criterion for classification of data as personal data or sensitive personal data. The security measures for the respective data are also provided. The rules along with the IT Act provides the framework for securing personal data. However, there are no definitions of metadata available. The Act or the rules do not provide any classification of metadata or any restrictions on the use of such data. There are no measures available for restricting the profiling of the user through the use of metadata.

The Personal Data Protection Bill replaces this framework. The bill provides an expansive definition of personal data by default. It includes profiling, collection of data which relates directly or indirectly to the person. The Bill provides a consent-based framework where the entity collecting data has to seek consent for collection and processing of data from the user. The Bill is on par with international standards on data collection and processing. But the exceptions provided under the Bill make such protection ineffective. The applicability of the Bill itself provides the first exception. The Act is made inapplicable when the data is processed anonymously. The exception also applies to government's processing of data and the collection and processing of such data for welfare measures. The Section 14 of the Bill provides exception to the consent-based model for processing of personal data. The exception is provided not only to the governments but also to the body corporates. The reasonable purpose as envisaged by the Bill includes the usage of such data for information and network security. The exception also includes collection of such data for fraud prevention. It is an expansive exception which would apply to any body corporate. The Section 15 provides for the government to categorise data as sensitive personal data. The categories of data classified as sensitive personal data are provided with additional protection, although, these cannot bypass the exceptions as well.

In this context, the metadata collected by WhatsApp Messenger which includes the mobile operator's name, battery level, etc. are anonymised data but are susceptible to use for profiling. The collection of data presently complies with the rules and the Act. It is in line with the security practices and procedures which are provided in the Act. In the Personal Data Protection Bill, the data collection is validated, taking into account all the exceptions provided under the Bill. In complying strictly with the Bill, the provisions may be violated but the expansive exceptions framework allows it to fly under the radar without any critical analysis under the Bill.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY