Privacy laws of digital India: Not enough to protect privacy

Introduction

The concept of privacy is often considered synonymous with that of confidentiality, but that is not the case. With booming e-commerce, it won't be wrong to say that "privacy" of individuals is not just about their privacy at home but applied in a much wider sense, including privacy of voice conversations, property, bank account, health records, passwords, photographs, business ideas, electronically transmitted communication etc.. In other words, privacy includes an individual's "data." Since the last few years, there has been an increasing traction in the field of data generation and processing, its storage and transfer and the pace at which incidents of data theft and intrusive surveillance are coming to limelight. Global corporations such as Google, Facebook and Amazon whose business model is based on the collection, storage and usage of customer data often land their customers in a vulnerable situation wherein their personal information gets commoditized by various other websites. With internet becoming all pervasive, there is a need to regulate the dealing of vast information stored therein and protect an individual's privacy.

This newsletter briefly throws light on jurisprudence on the subject, the limited privacy laws in India and the lacunae contained therein as well as the Personal Data (Protection) Bill, 2014 in the pipeline.

1. Judicial activism

The Constitution of India does not specifically grant the right to privacy, let alone data privacy. But fortunately, courts have time and again brought the right of privacy within the realm of fundamental rights and have opened gates for enacting laws on the subject.

For the first time, in Kharak Singh vs. State of U.P[1] where the petitioner was being harassed by the police through repetitive domiciliary visits at night, the Supreme Court equated personal liberty with privacy and observed that *"The right to personal liberty takes in not only a right to be free from restrictions placed on [his] movements, but also free from encroachments on [his] private life. It is true that our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty…the concept of liberty in Article 21[2] was comprehensive enough to include privacy and that a person's house, where he lives with his family is his castle and nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy".* Similarly, in another case of People's Union of Civil Liberties vs. Union of India[3], a voluntary organization had filed a public interest litigation before the Supreme Court to seek relief against indiscriminate and arbitrary telephone tapping of politicians done by various government officers in the shield of the provisions of the Telegraph Act, 1885[4]. The Supreme Court observed that *"It is no doubt correct that every Government, howsoever democratic, exercises some degree of sub rosa operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day."* The court deduced the right to life and personal

[1] AIR 1963 SC 1295
[2] Article 21 is included in Part III of the Constitution which contains fundamental rights
[3] 1995 SCC, Supl. (2) 572
[4] Section 5(2) of the Telegraph Act allows the government to intercept, detain and record transmissions in the interest of public safety.

liberty enshrined in Article 21[5] of the Constitution through an extensive interpretation of the phrase "Personal Liberty" and further observed that "*We have 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.*"

There have been many such precedents when the courts have, through various judgments justified the need to safeguard an individual's privacy. But, judicial activism has not really led to creation of a legal framework that matches the current business environment. The recent case of Karmanya Singh Sareen and Anr. Vs. Union of India and Ors[6] is a case in point and where a large key debate on privacy is centered currently. In this case, filed at the Delhi High court initially, the petitioners contended that WhatsApp Inc. (internet messaging application) cannot share users' data with Facebook Inc. Briefly, in August 2016, WhatsApp, pushed a notification to its users, asking them to accept recent changes in its terms and conditions. Many users agreed without checking the changes, and with that, unintentionally allowed WhatsApp to hand over information about them to its parent company Facebook for commercial use. This meant WhatApp's new privacy policy permitted it to collect and share information of its users with Facebook and all its group companies, including phone numbers and a user's contact list, in violation of the user's privacy. In the case at the High Court, the petitioners alleged "violation of fundamental rights of users" by sharing confidential information under the privacy policy. They contended that complete security and protection of privacy of the users details and data (an essential, significant and basic feature) was compromised under the new policy. To that end, they sought different writs and directions against the respondents[7] including, handling or dealing with personal data so as to ensure privacy rights are not compromised, formulation of guidelines to regulate functioning of the corporations involved, inform the users the true meaning of the privacy policy and protect minors. WhatsApp argued that the users gave their consent at the time of downloading the application in their smart phones upon hitting "I agree" to the application's terms and conditions. The petitioners countered and stated that while millions of users use the application daily, yet most of them are not literate to understand the full import and meaning of the privacy policy through which consent was given. The court, upon hearing the petitioners' argument acknowledged the violation of privacy but concluded that in the absence of a statutory framework for privacy, it cannot rule in favor of the petitioners' and will have to wait for the stand of the Supreme Court takes in another case of Justice K. S. Puttaswamy (retd) vs. Union of India[8]. The court further observed that if the user deletes the application from the phone anytime prior to September 29, 2016 then WhatsApp cannot share a deleted user's information. The petitioners, thereafter, approached the Supreme Court who has issued notice to the respondents. Given that serious privacy issues are involved, there is a likelihood that the case may eventually be heard by the Constitution bench. Be that as it may, it will be heard from May 12, 2017. In summation, pending a determination by the Supreme Court, as on date there is no restraint on WhatsApp to share the information.

[5] Article 21 is included in Part III of the Constitution of India and it contains certain fundamental rights.
[6] Decided by the Delhi High Court on September 29, 2016
[7] These included Union of India acting through Department of Telecom, What'sApp Inc. Facebook Inc., Facebook India and Telecom Regulatory Authority of India
[8] Writ Petition (Civil) No.494 OF 2016. In this petition a retired judge contended that collection of biometric data for Aadhar Card is an infringement of one's privacy, including vis-à-vis the government. The key issues that the court will hear are does the right to privacy occur and what are its contours and does an individual hold right to privacy against government too.

2. Current framework on data privacy

While the law on the subject is still evolving in the corridors of the court, the existing law on data privacy contained in the Information Technology Act, 2011 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Rules**") or the recently introduced Personal Data Protection Bill, 2014 ("**Bill**") remain inadequate to address the evolving landscape. The IT Act gives legal recognition to e-commerce and sections 43, 43A, 72 and 72A contain provisions which protect personal data[9] of a person.

Section 43 forbids downloading data without consent from the owner or a person who is in charge of a computer and prescribes punishment for introducing contaminant into a computer. Section 43A, read with the Rules, obligate corporations to adopt reasonable security practices for storing, dealing and disclosing sensitive personal data of an individual's sensitive personal data.[10] In case of lapses and where harm is caused to such individuals, there is a liability to pay damages. The definition of sensitive personal data is quite narrow. While putting together an all inclusive definition is not possible because what may be considered personal data by one may not be treated in the same manner by the other. Having said that, at least the definition could have been either more detailed or had the scope to include more aspects of personal information in its ambit. Further the Rules mandate corporations to adopt reasonable security practices for dealing and dissemination of sensitive personal data of a person and destroy the information, once the purpose is served.

Section 72 safeguards confidentiality of an individual's electronic records, books, registers, correspondence, information and documents. It prohibits those with access to such confidential data from disclosing to a third party and prescribes penalty for violation.[11] Section 72A protects an individual from dissemination of his personal information by a service provider including intermediaries. The provision prescribes heavy penalty[12] for accessing personal information of any person while providing services under a contractual obligation and thereby causing loss. However, again neither the IT Act nor the Rules define "personal information." So, while they ensure that the sensitive personal data of an individual is dealt with caution, ambiguity remains. On August 24, 2011, the Ministry of Information Technology issued a press note which stated that the rules 5 and 6 of the Rules, which provide for collection, storage, handling and dissemination of sensitive personal information to a third party, are applicable only to companies situated in India. The press note qualified that foreign companies dealing with sensitive personal data of an individual in India are not bound to adhere by the Rules. An inference could be drawn that foreign companies may share sensitive personal data with a third

[9] The IT Act defines "data" under section 2(1) (o) as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

[10] R.3 of the Rules defines sensitive personal data of a person as information related to password, financial information such as bank account or credit or debit card or other payment instrument details, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information or any detail relating to these which is given to a corporation for processing, storing in the context of services

[11] Imprisonment for up to two years and/or fine up to INR 1, 00,000 or about USD 1,500| USD 1= INR 67

[12] Imprisonment for up to three years and/or fine up to INR 5,00,000 or about USD 7,500

party anywhere in the world, unless it has contractually agreed otherwise. There is no rationale to this exemption, which was also affirmed by Ministry officials informally.

3. Framework under the Bill

The Bill seeks to provide protection of personal data and information of an individual and prevent from getting disseminated amongst other organizations. It was introduced in the Upper House of the Parliament on November 20, 2014 and so far, has not been passed. The Bill is not exhaustive and has merely 14 provisions. It does not define "privacy" but defines "personal data" as *information or data which relate to a living individual who can be identified from that information or data whether collected by any Government or any private organization or agency.* The Bill intends to protect privacy of an individual by the government and private organizations. Perhaps, this may extend to those outside India, though that is not stated clearly. The Bill has gone a step ahead as its provisions apply to all the residents of India and not merely citizens. It ensures that private bodies and government will have to adopt security measures while dealing with an individual's data. Further, the Bill suggests imposition of fiscal penalty (INR 5 million or about USD 75,000) on telecom service providers for misusing personal data of an individual. It is surprising to see that the Bill is not witnessing any movement since two years especially when India is focused on pushing the idea of "digital India".

Conclusion

India witnessed BPO boom few years ago, and that may have declined, but so far not faded. In fact, it has made India one of the biggest hosts of data outsourcing and has given it access to personal data of people around multiple jurisdictions. In the times when the Modi government is churning out digital surveillance projects such as Central Monitoring System,[13] DRDO NETRA[14]and NATGRID[15] it is ironical that the current legal framework to protect individual's privacy, let alone data privacy, is yet to come up to speed. Incidents such as selling phone numbers of girls in the state of Uttar Pradesh are being reported[16] and the recourse is merely to make police complaints which are many times ineffective. There isn't any law in the age of smart phones which expressly states that phone numbers qualify as personal data. It's high time that Indian government takes a cue from EU and realizes the importance of having a legal framework for protecting an individual's privacy. As the preamble to the EU Regulations 2016/679 issued by the European Parliament states

"The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."

Author
Mansi A. Gambhir

[13]Project to tap phone conversations, intercept e-mails and text messages, monitor posts on social networking service and track searches on Google

[14] This is a project to track online communications on a real time basis by harvesting data from various voice-over-IP services including Skype and Google Talk

[15] Project to connect databases of core security agencies of the Government

[16] This was reported by the Hindustan Times on February 3, 2017. News report available on- http://www.hindustantimes.com/india-news/girls-mobile-numbers-up-for-sale-in-uttar-pradesh-price-rs-50-to-rs-500/story-5lYPcav12h7rnW6A6UDLLI.html, web link last visited on February 21, 2017