Privacy in Internet Era

Kshitij Sinha
Amity Law School, Amity University
Haryana, India

ABSTRACT:

Internet has proved to be a boon in various ways but this also invites some issues of which one of the major ones is data protection and privacy. Privacy is not merely something which is to be traded upon, as if the data about us were currency and nothing else. It's a social property relating to values, culture, power, social standing, dignity, and liberty. Privacy is nowhere defined in law but major laws relating to this has been seen in Information Technology Act, 2000 and Indian Contract Act, 1872. Despite laws, India lacks in a proper legislative framework for data protection and privacy unlike developed countries like U.S.A, Russia, England where there are specific laws and legislative framework for combating data protection and privacy. The Battle for this started in 1954 with M.P Sharma's case and finally ended in Aadhar card's case in 2017 where the court incorporated the right to privacy under article 21 of the Indian constitution and made it a fundamental right. India being the largest host of outsourced data processing must have its own legislative framework to protect it. In 2013, National Cybersecurity Policy was drafted particularly in view of India's position as an exponentially growing business process outsourcing destination but this policy was stymied and even reasons were not made public. Further in 2017 Data Privacy Bill, 2017 was introduced but unfortunately it has still not been enacted into law. It is a very high time for the country to wake up as without proper legislation and strong cyber laws, data breaches and privacy cannot be controlled. The Data Security Council of India(DSCI) and Department of Information Technology(DIT) should also join hands and come up with the strong framework and should also work to spread awareness amongst people about the framework.

In Imagine, if we waived at someone and without our knowledge a high resolution camera clicks the photograph of our hand, capturing fingerprints of ours, what will happen? We might get upset, but on the contrary if we visit to a Disneyland kind of place where they make the image of our fingerprint to save us from waiting in the line, we might feel the novelty of the technology and the immediate benefits would be gratifying. Technology can be a boon or bane at the same time. Similar is the condition with internet in this modernizing and globalizing world.

In the age of hashtags, tweets, snaps, likes and shares, online privacy can seem almost non-existent. We are sharing our lives through social media now more than ever. If we are voluntarily handing over so much personal information, then the question arises that what's so important about online privacy? Most of the people assume that it's all about what they are doing but it is a very narrow picture. However, online privacy has more to do with who we are and what are we doing. Who we are refers to our personal identifiable information(PII) which as the name suggests- our name, number, date of birth, address, social security number, bank related information etc. and what are we doing refers to visiting a website or using a social media platform etc. and chances are always there that our private data might be leaked.

Privacy is nowhere defined in law but according to Black's Law Dictionary, right to privacy means "right to be let alone", the right of a person to be free from any unwarranted interference. The fight for right to privacy is

not recent in India. It started way back from 1954 when by an eight- judge bench in the case of **M.P Sharma vs Satish Chandra**[1], while dealing with the power to search and seize documents from Dalmia Group, dismissed the existence of right to privacy and further the case of **Kharak Singh vs. State of Uttar Pradesh**[2] where Supreme court again held that right to privacy is not a fundamental right. After going through all these battles over years, finally in 2017 in the case of **Justice K. Puttaswamy vs Union of India**[3] where the government of India decided to provide to all its citizens a unique identity called Aadhar which is card containing 12 digit Aadhar number. The registration for this card was made mandatory so as to enable the people to file tax returns, open bank accounts etc. However, the registration procedure to make such type of card required the citizens to provide their biometrics such as iris scans, fingerprints etc. Retired judge justice K.S Puttaswamy marched with the petition challenging the constitutional validity of this Aadhar project contending that there was an infringement of right to privacy of the citizens since, the registration for Aadhar is made cumpulsory. Therefore, all those who don't even want to register themselves, are not left with any option. Moreover, there is a deficiency of data protection laws in India and hence, there are chances that the private information of the people might be leaked if proper care is not taken. This will lead to infringement of right to privacy of the individuals. The supreme court held that Right to privacy is a fundamental right, subject to reasonable restrictions. However, it is evident that privacy cannot be an absolute right. For instance, surveillance is important to prevent the crime in the society. An individual cannot just argue that his privacy is being violated if larger public interest requires keeping him/her under the surveillance.

After this case a major question arose that why India expressly does not have any legislation governing the data protection or privacy. However, relevant laws in India dealing with data protection or privacy are Information Technology Act, 2000 and the Indian Contract Act, 1872. The issues that are linked to the payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and infringement of contractual terms in respect of personal data is mentioned under the Information Technology Act, 2000

Under section 43A of the Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining rational security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is essential to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,

[1] 1954 SCR 1077
[2] 1964 (1) SCR 322
[3] (2017) 10 SCC 1

2011 which is notified by the government deals with the security of "Sensitive personal data or information of an individual", that provides the personal facts relating to:

- Passwords;
- Financial information such as bank account details, credit card, debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information.

These rules deal with the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possesses, stores, deals or handles information is necessary to follow while dealing with "Personal sensitive data or information". If there is any breach, the body corporate or any other person acting on behalf of body corporate, the body corporate may be held liable to pay damages to the person so affected.

The disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to RS 5,00,000 is provided under section 72A of the Information Technology Act, 2000

It should be noted that section 69 of the Act, which is an exception to the general rule of maintenance of privacy and secrecy of the information, provides that where the Government is satisfied that it is essential in the interest of:

- The sovereignty or integrity of India,
- Defense of India,
- Security of the State,
- Friendly relations with foreign States or
- Public order or
- For stopping incitement to the commission of any cognizable offence relating to above or
- For investigation of any offence,

It may by order, instruct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. This section gives the power to the Government to intercept, monitor or decrypt any information including information of personal nature in any computer resource. Where the information is such that it is ought to be disclosed in public interest, the Government may require disclosure of such information. Information involving anti-national activities which are against national security, breaches of the law or statutory duty or fraud may come under this category.

Another major question arises here is that despite India has so many laws on data protection and privacy then, why India lacks to ensure data protection and privacy. This is due to absence of a proper legislative framework for data protection and privacy. Authorities constituted to regulate compliance and enforce penalties for non-compliance under the Information Technology Act, 2000 and the Information Technology (Amendment) Act, 2008 have been inactive for years and a very little significant jurisprudential development has occurred on the subjects of cybersecurity, privacy and data protection over the past few years. In 2013, the government drafted a National Cybersecurity Policy, which generated considerable interest both in India as well as abroad, particularly in view of India's position as an exponentially growing business process outsourcing destination. Sadly, the progress on the policy was stymied for reasons that have not been made public, reflecting rather poorly on the government's intention to provide clear, robust and watertight law on these matters. Further in 2016, Joint Secretary for Cyber Laws and E-Security, R.K Sudhanshu, stated to the press that the government is in the process of developing new encryption and cybersecurity policies as part of a thorough overhaul of the law regulating cybersecurity in India. Again in 2017 Minister for Law and IT, Ravi Shankar Prasad, said that the government is finalizing cybersecurity standards for mobile phones and has already issued notice to most smartphone manufacturers asking them to furnish details related to cybersecurity followed by introduction of Data Privacy Bill, 2017 but unfortunately it has still not been enacted into law. If we compare it to various developed countries then, it is evident that to combat data privacy developed nations have their laws like U.S.A has Privacy Act, 1974 and Electronic Signatures in Global National Commerce Act. England has Data Protection Act, 1998, Electronic Communication Act, 2000 and Network and Information Systems Regulations of 2018. Russia has Federal Law No. 63-FZ on electronic signatures, Federal Law No. 149-FZ Information, Information Technologies and Protection of Information and Federal Law Regarding Personal Data 2006.

Data protection law in India is facing many problems and resentments due to the absence of appropriate legislative framework. There is ongoing explosion of cybercrime, leaking of data etc. on a global scale. The theft and sale of stolen data is ongoing across vast continents where physical boundaries pose no restriction or seem non-existent. India being the largest host of outsourced data processing in the world could become the

epicenter of such cybercrimes. This is all due to lack of appropriate legislation. The Data Security Council of India(DSCI) and Department of Information Technology(DIT) must also apply its efforts in this regard and similar lines. However, the best solution can come from good legislative provisions along with the suitable public and employee awareness. It's high time to wake up when even PMO's cyber security is compromised for several months. Data breaches and cybercrimes cannot be reduced until we make strong cyber laws. We cannot achieve so by merely declaring a cat as a tiger. Therefore, cyber law of India must be supported by sound cyber security and effective cyber forensics.