Volume 17, November 2021 ISSN 2581-5504

"Data Breach and Privacy with Special Emphasis on Corporate Sector"

Sanya Pahouja
Vivekananda Institute of Professional Studies

Abstract

This research paper deals with a current topic-data breach and Privacy with special emphasis on corporate sector . The researcher has focused upon the need of a centre level comprehensive law on data privacy as the lack of same has been the real reason behind incidents like Aarogya Setu data issue or the Whatsapp data leak case which have been discussed hereby in brief . IT Act, 2002 which deals with data protection has been mentioned as a passing reference and due emphasis has been laid on the Companies Act , 2013 . Data privacy laws from the UK and US have been discussed in brief and the same have been contrasted with the Indian laws.

Keywords: data, breach, privacy, information, laws, Companies.

Introduction

In the current era of globalization where value and volume of data is constantly increasing due to increase of trade , the issue of data privacy has acquired newer paradigms . Unlike earlier , ensuring data privacy is not a matter of advantage over the competitors any more , rather , it is now acquired a legal status round the globe .[1] Regulators and market place exert much pressure on the companies so that they improves their data collection process , usage and storage of all personal information and data and most importantly its deletion . With the advancement of internet , data privacy has become more important than ever . Until much recently , the data protection efforts of several businesses have revolved around the special laws and standards prescribed for their particular sectors . However , give the present conditions , such industry specific data policies were no longer helpful . Businesses will benefit from a more systematic and organized approach to Information governance which must be motivated by the increased significance and awareness of the data protection concern , as well as by the sweeping data regulations . Large business houses , particularly those doing global business , require an elaborate management of compliance that encompasses within itself all related business processes . The design and execution of company-wide enforcement and data collection systems must be in tandem with cross-border legal standards , particularly with data privacy legislation , in order to maintain the trust of their clients and staff and to minimize the liability risks of their directors and officers .

In India , the right to privacy has been elevated to the standard of fundamental rights as under the case of Justice K.S. Puttaswamy (Retd) v Union of India[2], right to privacy came to be included within the ambit of Article 21 of the Constitution of India , 1950 . As such , the

[1] "Data privacy as a strategic priority:, Deloitte (February 18, 2021,05:00 am) https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-data-privacy-as-a-strategic-priority.pdf
[2] Ibid.

Volume 17, November 2021 ISSN 2581-5504

Indian judiciary has granted supreme value to the right to privacy and it can only be constrained for legitimate purposes , such as state protection and the public interest .[3] In India , there is currently no clear law dealing with the security of data and records . Data and privacy rights can be obtained from separate legislation relating to information technologies , intellectual property rights , criminal law and contractual relationships . In regards to data from information networks , the IT Act allows for protection from such violations . The said legislation includes provisions for the prevention of illegal use of computers , operating programs and data stored in them . The Indian Penal Code , 1860 does not expressly discuss data security abuses and violations . Under the Indian Penal Code , 1860 , responsibility must be inferred from relevant offences for such violations. For example , for fraudulent misappropriation or conversion of "movable property" for one's own usage , Section 403 of the India Penal Code imposes jail sentences and appropriate fines . The Indian Copyright Act prescribes mandatory punishments for misusing copyrighted material . As per the CICRA that is the Credit Information Companies Regulation Act , 2005 , credit information relating to people in India must be obtained in consonance with the privacy requirements set out in the CICRA Law .[4] India has been following the EU's General Data Protection Regulation (GDPR) and has thus allowed global companies to carry out their business subject to some terms and conditions instead of resorting to the Chinese framework which prevents multinational companies like Facebook and Google from operating in the country .[5] The Indian government has proposed a Personal Data Protection Bill (DPB) , 2019 which would regulate the collection , protection and disclosure of personal data of residents of India .

Current Data Protection Laws and Corporate Sector

Since India lacks a comprehensive and special law which deals with data security , there are a number of legislation(s) from which the law is derived . India is not a member to any agreement like the GDPR or the Data Protection Directives relating to the protection of personal information and data . India , however , has consented or is a member to other international treaties that uphold the right to privacy like the Universal Declaration on Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) . The Information and Technology Act, 2000 was amended to include Section 43A and Section 72A . These sections laid down the right to recovery for unauthorized disclosure of personal information .[6] After some time , u/s 43A of the IT Act, 2000 the centre government formulated the Information Technology (Reasonable Protection Standards and Procedures and Confidential Personal Data or Information) Regulations, 2011 . A set of clarifications of these rules was released on 24 August , 2011 . Specific provisions have been levied by the regulations on commercial and private organizations in India relating to the storage and

[3] (2017) 10 SCC 1.
[4] "Data Protection and Privacy Issues in India", EPL:Advocates and solicitors (February 18, 2021, 05:00 pm) https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf
[5] Vijay Govindarajan, Anup Srivastava, and Luminita Enache, "How India Plans to Protect Consumer Data", Harvard Business Review (February 20, 2021, 04:00 am)
[6] Supra note 4.

dissemination of confidential private details or information which is at par with the General Data Protection Regulation (GDPR) and the Data Security Directives . India has no central Personal Data Privacy Regulation Body . It is the responsibility of the Ministry of Electronics and Information Technology to enforce the IT Act and issue the regulations and other explanations under the IT Act .[7]

When the question of data protection related to corporate houses comes into picture , it is unfortunate to note that the Companies act of 2013 is silent on data privacy and data protection . However , there are certain provision in the law which are often referred to in cases of data privacy violations especially when the topic of liability of the directors comes into play as far as data protection and privacy is concerned . A "director" is regarded as "a director appointed to the company's board" in accordance with Section 2(34) of the Companies Act, 2013 . The controller of the company's affairs is a director . There were no clauses for the legislative duties of directors in the Companies Act, 1956 , and it was controlled by the minimum standards of the board and precedents . The duties of the director are provided for in Section 166 of the Companies Act, 2013 and are listed below :

1. The director shall act in consonance with its terms of association (AoA) .
2. The director must act in good conscience to uphold the interests of the enterprise for the betterment of stakeholders as whole in the larger interest of the enterprise , its workers , its owners , society and the even the surrounding ecology .
3. With due care , skill and diligence , the director shall exercise his duties and give sound judgement(s) .
4. The director shall not take part in any decision where it may have even an iota of interest or stake which interferes with , or is likely to interfere with , the company's interest .
5. No undue gain or benefit must be achieved or even attempted to be achieved by the director for himself and also his relatives , partners or associates and if such director is found liable of incurring any unlawful gain , he shall be held responsible for paying an amount equivalent to such gain to the company .
6. The director must not assign his office and any such assignment if made shall be declared to be void .

It is essential to note that all the duties of the director can be divided into two broad categories namely :[8]

1. Duty of Care , skill , diligence and independent judgment .
2. Fiduciary duties .

It is essential to understand the implications of Section 166[9] so that the impact of same on data privacy can be better interpreted . Some of the implications are discussed below :[10]

[7] Supra note 4.
[8] Ifla A,"Codification Of Duties Of Directors Under The Companies Act 2013", Mondaq (February 20, 2021,10:00 am) https://www.mondaq.com/india/corporate-governance/695304/codification-of-duties-of-directors-under-the-companies-act-2013
[9] The Companies Act, 2013.

Volume 17, November 2021 ISSN 2581-5504

1. Important role of discretion : The applicability of a director's discretion must be well established and focused upon an in-depth review of all pertinent facts .
2. Full disclosure of relevant data , that is , information upon which a decision is made .
Violation of section 166[11] is an offence punished by a penalty of not less than one lakh , but which can stretch to 5 lakh INR . However , if a director is guilty of making an unfair profit , he will then be responsible for paying a sum equal to the profit to the corporation .

The Companies Act, 2013 was enacted to repeal the aged Companies Act of 1956 as that law was not suited to the present day requirements of corporate world . Unfortunately the law makers failed to include an extremely important issue of the corporate in the state which is that of data security and breach of data . However , the codified duties of the directors under Section 166[12] have been interpreted so as to include instances of cyber security and data breach within their ambit . It is within the header of duty of care , skill and diligence that cyber security and data breach are included . The general perception that appropriate data protection measures should be part of the rational care that any director must exercise in handling corporate risk is difficult to negate in today's world .[13] However as per law , whether this perception is valid or not is still unclear . In deciding upon this question , the judicial authorities are bound to take note of the following factors :[14]

1. Technology of the company's existing organizational and technological framework ;
2. Principles and risk management specific to a business and sector ;
3. Level of arguments taking place on cyber security and data breach at board or committee level ;
4. Application of guidelines at organizational level .
5. Auditing and certification of security processes by a third party ; and
6. Background and possibility of retention of earlier events .

In addition to the directors' duty to maintain cyber protection as part of their fiduciary responsibilities under Section 166[15] , certain instances of delegated legislation provided under the Act impose certain express data security obligations which are to be followed by the management . Section 28(1) of the Companies (Management and Administration) Rules , 2014 grants responsibility for preservation and protection of electronic data and documents to the managing director , company secretary , or other appointed officers or agents . Section 28(2) of these regulations specify certain specific responsibilities of the management with regards to the current topic and the same have been enumerated below :[16]

---

[10] Supra note 8.
[11] Supra note 9.
[12] Supra note 9.
[13] Kevin LaCroix, "Guest Post: Cybersecurity and D&O Liability: Emerging Concerns under Indian Law", The D&O Diary (February 17, 2021,03:00 pm)
https://www.dandodiary.com/2018/05/articles/international-d-o/guest-post-cybersecurity-liability-emerging-concerns-indian-law/
[14] Ibid.
[15] The Companies Act, 2013,
[16] Supra note 13.

Volume 17, November 2021 ISSN 2581-5504

1. Protecting sufficiently against any form of illegal access , deletion or misuse of data ;
2. Lack of documents as a consequence of disruption to or malfunction of the system in which the data is kept ;
3. In order to guarantee accuracy , sustainability and consistent performance , computer systems, software and hardware are duly protected and evaluated .
4. Records that are precise , usable and reliable of being replicated further for reference ;
5. That a minimum one copy of modified documents held in electronic form is taken at a pace not beyond a period of one day ;
6. Appropriate measures are to be taken to ensure the security , honesty and privacy of information ;
7. Restriction on access to data to the managing director , company secretary or any other director or officer or persons as authorized by the Board on its behalf ;

Under the aforesaid rules , the meaning of the term electronic records is given as - " data, record or data generated , image or sound stored , received or sent in an electronic form or micro film or computer generated micro fiche ." The fine imposed for non-compliance of the aforesaid rules is minimal , notwithstanding the express acknowledgement of the duty of directors to ensure data protection . Any failure to comply may result in fines that may range up to INR five thousand and if the violation is of an ongoing kind , another such fine may be increased to INR five hundred rupees per day after the first day on which the breach had begun . In situation of data breach , whether class action suits can be a viable method for affected investors to get rightful compensation needs to be asserted .[17]

Indian Judiciary on Data privacy

The courts in India have dealt with the issue of privacy in a number of cases . In the case of Justice KS Puttaswamy (Retd) v Union of India[18]. Justice Chandrachud and Justice Bobde remarked :[19]

> "At a normative level privacy subserves those eternal values upon which the guarantees of life , liberty and freedom are founded . At a descriptive level , privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty ."

In R. Rajgopal and Ors v State of T.N[20], the Apex recognized a person's right to safeguard his privacy in a plethora of matters. In People's Union of Civil Liberties v UOI[21], , the right to privacy was recognized in the light of Art 17 of the International Covenant on Civil and Political Rights and Art 12 of the Universal Declaration of Human Rights . In Ram Jethmalani and Ors v UOI[22], the SC recognized the right to privacy as an integral part of Article 21 of the Constitution of India , 1950 . The Right to Privacy is a fundamental right

[17] Supra note 13.
[18] Supra note 3.
[19] Supra note 3.
[20] 1995 AIR 264.
[21] (1997) 1 SCC 301.
[22] (2011) 1 SCC 560.

covered within the ambit of right to life and personal liberty under Article 21 which can be curtailed via procedure established by law which is just, fair and reasonable as laid down in Maneka Gandhi v Union of India[23]. In State of Maharashtra v Bharat Shanti Lal Shah[24], the Supreme Court laid down that the right to privacy can be curtailed in accordance with the procedure validly established by law . In Govind v. State of Madhya Pradesh[25], it was held that the fundamental right explicitly guaranteed to a citizen has plethora of zones zones and that the right to privacy is itself a fundamental right , and it must be subject to restriction on the basis of compelling public interests . From all the case laws discussed , it is clear that the the Indian judiciary has developed the concept of privacy as a wide term . Privacy is to be understood in a wide sense- it includes bodily autonomy , making choices in matters understood as being personal and off course one's personal information . Being encompassed within the limit of Article 21 of the Constitution of India , 1950 , right to privacy can be curtailed only in exceptional circumstances that is in lieu of compelling state interest and if it fulfills the benchmark of proportionality test laid in the Puttaswamy judgment .

Liability of Directors in Data breach cases

As per the test of proportionality , for the purpose of determining the reasonableness of any restriction or infringement of right to privacy there are three yardsticks which are :

a. Legality of the restriction posed : Must be backed by legislature .

b. Suitability and Necessity of the restriction for larger good .

c. extent of interference must be proportionate to the need for such interference to meet the larger good .

Therefore in light of all the above explanations , it is clear that the right to privacy includes the right to protect private data and thus the yardsticks which are to be fulfilled for curtailing the right to privacy including privacy of personal data must be fulfilled by anyone who is doing so . It thus includes directors of various companies within its ambit . It is to be understood here that when a company commits any breach be it related to data privacy , the director shall be liable when :[26]

A) He or she at the time of commission of the offense was responsible for the carrying out of business of the corporation ; or
B) He or she whose consent and negligence was reason for the commission of the offense .

[23] 1978 SCR (2) 621.
[24] (2008) 13 SCC 5.
[25] 1975 AIR 1378.
[26] Vyapak Desai and Ashish Kabra, "Director and Officer Liability in India", Nisthi Desai and Associates (February 20, 2021, 07:00 am)
http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Articles/Director_and_Officer_Liability_in_India.pdf

Volume 17, November 2021 ISSN 2581-5504

Under Section 150(12)[27], an independent or non-executive director is responsible only for actions of omission or commission by any corporation that happened with the approval of such director or the permission or full cooperation of the director or in cases where he or she refuse to perform faithfully . This, to some degree , mitigates the question over independent director responsibility . However , certain questions still remain unanswered like- whether a director behaved faithfully and whether information may be traced to a director by mere attendance at board meetings . In addition , responsibility incurred under numerous other enactments by independent and candidate directors remains a valid issue . Acts including dishonor of cheques under the Negotiable Instruments Act, 1881 , violations underneath the Income Tax Act, 1961 , infringement of currency exchange laws , infringement of securities rules , non-payment of provident fund payments , etc may result in liability that may not always be limited to the executive directors . Additionally , certain statutes dealing with related matters make no distinction between the different types of directors in a company . The Honorable Supreme Court in the cases of Nat'l Small Indus. Corp. Ltd. v. Harmeet Singh Paintal & Anr[28] and K.K. Ahuja v V.K. Vora[29] has held that it is the managing director or MD who is prima facie in charge and responsible for the business of an enterprise and can be sued by the company for commission of misdeeds .

As inferred from the entire discussion , the liability of the directors of the company in matters of breach of data privacy shall be at par with the liability of directors in all other matters since data breach is within the ambit of director's duty of maintaining due care and diligence .

Data Breach and Privacy in Other countries

The author has referred to the data breach and privacy related law as followed in the United Kingdom and the United States .

United Kingdom

The Data Protection Act , 2018 regulates as to how one's personal information is to be used by organizations and the government . The Data Protection Act , 2018 is United Kingdom's extension of the General Data Protection Regulation (GDPR) which is followed in all member countries of the European Union (EU) . All liable for using personal data must obey specific guidelines called 'principles of data security' . They must make sure that the data is :[30]

1. Reasonably , legally and transparent used .
2. Used for well defined purposes only .
3. Used in such a way which is acceptable and such usage is restricted within the ambit of necessity .

[27] The Companies Act, 2013.
[28] (2010) 3 S.C.C. 330 .
[29] (2009) 10 S.C.C. 48 .
[30] https://www.gov.uk/data-protection

Volume 17, November 2021 ISSN 2581-5504

4. Precise and if possible also up to date .
5. Not retained for such time period after its requirement ceases .

One is enabled to be acquainted with what knowledge the government and other institutions keep on one as per the Data Security Act , 2018 . These includes the right to :

1. Be aware of the use of one's personal data .
2. Access personal data .
3. Make changes if data being used is wrongful .
4. Get the data deleted .
5. Ceasing and Prohibiting the transmission of one's data .

One gets some sort of protection if an agency utilizes his or her personal details for:[31]

1. Procedures relating to automatically making of decisions (without involving humans) .
2. Profiling , like anticipating one's actions or wishes .

Following are some of the recent case laws of data and privacy breach in the United Kingdom :

1. LLoyd v Google LLC[32] : This is a significant ruling with substantial consequences for the regulation and application of data security in United Kingdom . This representative argument , made on behalf of an estimated 4.4 million iPhone users , involves the compilation and manipulation of browser generated information ('BGI') by Google on Apple's Safari web browser . In this case , it was held that a representative lawsuit (supported by a litigation funder) can be a reasonable and effective mechanism to be used when suing for damages in relation to a multi-person violation of privacy protection legislation .
2. R (Bridges) v Chief Constable of South Wales Police and Others[33]: It is a latest case law whereby the UK Administrative court ruled in favour of the software used by the police for making facial recognition . The court in this case laid down several essential points and some of the important ones have been discusses below :

a) Any usage of facial recognition technology has to undergo a Data Protection Impact Assessment which should make the assumption that privacy rights under the European Convention on Human Rights are likely to be infringed by the use of the technology .

b) The advantages obtained by using facial recognition technologies will overshadow the privacy rights of a person . Such advantage would be specific from case to case and in this case the usage of the police was found to be proportionate by the court .

c) The technology of facial recognition interferes with the privacy of a person so all usage must be legitimate in the eyes of law . Although , the general application of the device was fair , it is impossible under law to allow freedom as to when to use it until and unless certain extremely clear guidelines are laid on the same ,

d) In this case , legislation dealing with equality in public sector was included . While this shall not be the case with organizations from private sector , the courts have clearly been

[31] Supra note 30.
[32] [2019] EWCA Civ 1599.
[33] [2019] EWHC 2341 (Admin).

open about the possibility of discrimination and it is rather expected from the users of such systems to satisfy themself that there will be no biasness .

United States

Quite surprisingly , it is noted that United States has no data protection laws . There is no law at the Centre which shall deal with data privacy and breach at the central level unlike the GDPR law of the European Union . There are instead several laws dealing in privacy issues like privacy laws focused upon consumers enacted in various states of the country .[34]Somewhat like the Companies Act of 2013 in India , one has the Federal Trade Commission Act in the United States . Within its jurisdiction , the Federal Trade Commission Act has immense power over private enterprises to avoid discriminatory or deceiving marketing practices . Although , the FTC does not specifically dictate what data can be used in privacy policy for websites , it uses its power to impose rules , implement privacy laws , and take compliance steps to protect the consumers . FTC has often taken actions against the companies in matters of data privacy :[35]

1. On the occasion of failure to impose and maintain various measures relating to data security .
2. Failure to adhere to the relevant self regulatory standards of the business of the company .
3. Failure in adhering to a privacy policy which has been published .
4. Dissemination of data in undisclosed mannerisms .
5. Misleading the consumers by supplying them with wrongful information regarding usage of their data .
6. Failure to keep the personal information of the consumers secured from instances of data intrusion .
7. Violating the privacy rights of consumers by way of collecting , tackling , or exchanging their data is an infringement of the privacy benchmark set by the FTC or of the rules and regulations of national privacy .
8. Indulging in unlawful and unethical marketing practices .

Famous Data Breach Cases in India

Due to the lack of any comprehensive law on personal data protection in India , there have been large scale violation and non adherence to the otherwise prevalent dictates on data privacy in the country . Two of the recent and most famous instances of data breach have been discussed hereby :

[34] Andy Green, "Complete Guide to Privacy Laws in the US", Varonis (February 19, 2021, 08:00 pm) https://www.varonis.com/blog/us-privacy-laws/
[35] Supra note 34.

A) Aarogya Setu Data Leak Case[36]

The Aarogya Setu smartphone application was launched during the Covid-19 pandemic as India's technical tool to fight against the latest Coronavirus outbreak, . The App focused on contact tracking and ensured that it assists persons who are likely to be carriers of the disorder or are susceptible to the disease as they have come in contact with a Covid positive person or have visited any such area where such person was present . While the former contact tracing techniques involved physical interviews with people , mobile technology has made the process a lot easier . However , the use of such apps has raised a host of questions regarding privacy. There have been several questions about the massive data gathering and its usage since the publication of the app , particularly in the absence of any specific legislative mechanism to resolve these growing concerns . However the issue escalated when it was made mandatory for everyone going for work and present in the containment zones to install the Aarogya Setu app . This lead to an influx of a number of writ petitions being filed regarding the constitutionality of the app in the Kerala High Court . Interestingly , the Honorable Kerala High Court refrained from deciding upon the constitutionality of the app but asked the centre to look upon its act of imposing the usage of such app . Consequently , the use of this application was made voluntarily .

The Aarogya setu app has been heavily criticized for been violative of the proportionality test laid down in the Puttaswamy case(supra) . Firstly , the application is not backed by any legislation . Secondly in absence of any data protection law in the country , there can be no credibility or assurance regarding the safety of data being taken while using the application . Thirdly , on the basis of data of similar contact tracing apps used in other countries , it is inferred that such acts have no paramount job in controlling the pandemic . Hence this application does not fulfill the third yardstick of necessity as laid under the proportionality test . Other factors like lack of transparency , ambiguity in privacy policy , etc are also responsible for raising questions upon the credibility of the application .

B) Whatsapp data leak case[37]

Whatsapp is the most widely used social media platform in our country and rightfully the most controversial one also . Whatsapp groups have been misused by many people in furtherance of illegal activities . However , the most classic example of misusing the social media platform is said to be SEBI data leak case . During the November of 2017 , the Security and Exchange Board of India (SEBI) noticed the various media reports which were talking about circulation of unpublished price sensitive information (UPSI) on various private WhatsApp groups about certain corporate houses in much advance of the official information

[36]Priyam Jhudele and Shantanu Pachauri, "Aarogya Setu: An analysis of the Data Access and Knowledge Sharing Protocol, 2020", Bar and Bench (February 20, 2021, 07:25 pm) https://www.barandbench.com/columns/an-analysis-of-the-data-access-and-knowledge-sharing-protocol-2020

[37] Vijay Parthasarathi, Rohan Banerjee & Rohit Tiwari, "SEBI and WhatsApp leaks: Every link in the chain matters", Cyril Amarchand Mangaldas Blog (February 17, 2021, 07:11 pm)https://corporate.cyrilamarchandblogs.com/2020/06/sebi-and-whatsapp-leaks-every-link-in-the-chain-matters/#:~:text=After%20examining%20the%20WhatsApp%20chats,the%20subject%20matter%20of%20the

Volume 17, November 2021 ISSN 2581-5504

being given to the stock exchanges .[38] The regulator placed market managers , trading houses , auditors , consultants , financial consultants and business leaders under the scrutiny . Provisional orders were released against many big firms allegedly published by UPSI , with the regulator trying to take a stern stance on businesses that did not address corporate accountability for any leaks . SEBI directed all such organizations to conduct inquiries internally to find those responsible for the leak , to take measures to verify any recurrence , and to supply SEBI with the necessary information . Unfortunately , these businesses replied to these internal leaks with clean chits , and SEBI was thus unable to locate the initial source of this entire data leak case . However , SEBI intensified the entire investigation , undertook a search and seizure operation involving 26 individuals who were involved in the 'Market Chatter' WhatsApp community (main Whatsapp group involved in the controversy) and seized around 190 relevant computers and documents .[39]

This case is one out of the huge number of data privacy issues which have arisen in relation to Whatsapp . In absence of uniform data protection law in India , Whatsapp has managed to escape from the clutches of law almost every time . The most recent example is that of the controversial Whatsapp policy which will in all probability be implemented in India by May 2021 while in EU due to the presence of comprehensive data law , such policy will not be implemented .[40]

Comparative Analysis Between Data Privacy between India, UK and USA

Out of these three countries , it is only the United Kingdom which has a central law on personal data protection . It is surprising to note that United States despite being the land of origination of Facebook and Whatsapp has no central level legislation on data privacy . The law on the issue varies from state to state in the country . However , FTC acts a national level body for tackling data privacy issues concerning the business world . Hence this situation as prevalent in India is much more sad and appalling as India neither has central level data protection laws , state level data protection laws or a central level authority which deals in this issue . UK has its own data protection law making it easier to establish to culpability and so is the case in US due to presence of state level laws . In India , it is the judiciary which has propounded upon the subject of privacy a number of times and the same has developed to form perceptions on data privacy . The Companies Act of 2013 and the associated rules indirectly deal with data privacy but the same does not suffice the needs of the Indians and their data privacy issues . The role played by FTC in US might be considered to be like what is of the Companies Act in India . However , FTC shall be much more effective , that is , it a regulatory body of corporate matters while in India the provisions of the Act shall be imposed by the courts which are already suffering from the issue of back logs .

[38] Ibid.
[39] Ibid.
[40] Ibid.

Volume 17, November 2021 ISSN 2581-5504

Conclusion

In the current era of globalization , it has become much easier than it was ever earlier to save and transfer data . However , this have had not only positive results but also several negative implications which are evident from the Aarogya setu case and Whatsapp data leak case . It has become easier to exploit data and breach the privacy of the masses . Since it is a relatively new concern , there is no concrete law on the topic . The Personal Data Protection Bill of 2019 was introduced in the Parliament as an attempt to bring in a comprehensive centre level law on the issue but the same has not yet become a reality . Data privacy is extremely important in all spheres of life but most importantly in the corporate world . section 166 of the Companies Act , 2013 has been interpreted to serve the needs of data privacy and establish the liability of directors in such cases . However , whether the lawmakers actually intended of interpreting the statute in such manner is best known to them only . India needs to take the issue seriously as it is not at par with other leading nations of the world when it comes to data privacy issues .