BIG DATA TECHNOLOGY- A PARADOX TO CONTEMPORARY CONSUMER'S CONSENT IN THE GLOBAL MARKET

[*]Dhruthi C & [**]Hima M

ABSTRACT

The global market is known for its inclusion of the latest technologies and progression towards a better approach to consumers. With this shift in the market, the meaning of a 'consumer' has become sophisticated. It has also resulted in various fallacies and one such concern is the concept of Big Data with respect to the privacy of consumers. Irrespective of whether there is consumer's consent, corporate companies, governmental agencies and foreign organizations have access to their personal information. It can be evolved into valuable data, which is used for various purposes, other than using it for keeping a track for marketing purposes. A policy as such must be formulated which balances the functioning of the market and protects the rights of consumers. The paper throws light upon the necessity of a specific policy to deal with the modern problems and inclusion of technology in policy making. In a nutshell, an interdisciplinary approach is adopted to discuss the need to protect the interests of consumers in the present market conditions and dynamically changing attitudes.

I. BIG DATA- A CONTEMPORARY CHALLENGE

As our society grows more complex, interconnected, and technologically advanced, data is generated that reflects this societal change, and potentially allows us to better understand this complexity.[1] The whole process of data collection itself has become a pivotal target for companies and other institutions to increase their profits and scrutinize their businesses. Perhaps, the collection of data related to consumers is an outlook of business strategies in today's global market.

[*] Dhruthi C, 3rd year, BA. LLB, JSS Law College, Autonomous, Karnataka.
[**] Hima M, 3rd year, BA. LLB, JSS Law College, Autonomous, Karnataka.

[1] G. West, *Big Data Needs a Big Theory to Go with it*, SCI, available at https://www.scientificamerican.com/article/big-data-needs-big-theory/., last seen on 21/10/2020.

The above idea was conceptualized into a reality through the advent of Big Data technology. Big Data may involve personal data: that is, any information relating to an individual, and can be anything from a name, a photo, an e-mail address, bank details, posts on social networking websites, medical information, or a computer's IP address.[2]

The European Commission defines Big Data as: *"Large amounts of different types of data produced from various types of sources, such as people, machines or sensors. This data includes climate information, satellite imagery, digital pictures and videos, transition records or GPS signals."*[3]

Thus, with technology, every individual's movements, decisions, and purchases—every recordable detail of their lives—is captured and memorialized in the electronic realm. Due to the exponentially increasing efficiency of storage, the data is collected in centralized servers, stored, and analyzed in other ways that were never before possible.[4]

Data, in its raw form is obtained through numerous ways, which includes collection through websites, cookies, social media, company records and so on. Many a times, the consumers are either unaware or negligent, and end up providing information that is needed and expected by such institutions.

The age of information has resulted in complex issues for informational privacy. These issues arise from the nature of information itself. Information has three facets: it is not rivalrous, invisible and recombinant. Information is not rivalrous in the sense that there can be simultaneous users of the good – use of a piece of information by one person does not make it less available to another. Secondly, invasions of data-privacy are difficult to detect because they can be invisible. Information can be accessed, stored and disseminated without notice. Its ability to travel at the

---

[2] Director General for Justice and Consumers*, The EU Data Protection Reform and Big Data: Factsheet 2016*, Commission Europe, available at https://publications.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1, last seen on 21/10/2020.

[3] Ibid.

[4] C. Devins, T. Felin, S. Kauffman & R. Koppl*, The Law and Big Data*, 27 Cornell Journal of Law and Public Policy 357, 363 (2013), available at https://www.lawschool.cornell.edu/research/JLPP/upload/Devins-et-al-final.pdf, last seen on 12/11/2020.

speed of light enhances the invisibility of access to data, 'information collection can be the swiftest theft of all'. Thirdly, information is recombinant in the sense that data output can be used as an input to generate more data output.[5]

Thus, complex steps are involved in constituting Big Data owing to its volume, velocity, variety and value. The data collected shall be sorted and the important statistics shall be extracted (also known as data mining). Such valuable insights shall be stored for further analysis and extraction. The data analysis is the crucial phase, wherein such valuable information shall be further divided into many databases, each under different categories of studies associated with behavioral pattern, reasoning and approach towards market conditions and changes. Thus, what seems to be plain information for a layman, holds beneficial value for associated businessmen and other functionaries.

With the advent of the Internet of Things (**"IoT"**), more objects and devices are connected to the internet, gathering data on customer usage patterns and product performance. The emergence of Machine Learning (**"ML"**) has produced still more data. While Big Data has come far, its usefulness is only just beginning. Cloud computing has expanded Big Data possibilities even further. The cloud offers truly elastic scalability, where developers can simply spin up ad hoc clusters to test a subset of data.[6] The development and extensive use of highly distributed and scalable systems to process Big Data is widely considered. New data management architectures, e.g., distributed file systems and NoSQL databases, are used in this context.[7]

Thus, advancement in the field of Big Data is an ongoing process with the improvement in technology, science and research. Though it's a beneficial

[5] C.P. Moniodis, *Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy*, 15 (1) Yale Journal of Law and Technology, 139, 153 (2012), available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1080&context=yjolt, last seen on 20/10/2020.
[6] *The definition of Big Data*, Oracle, available at https://www.oracle.com/in/big-data/what-is-big-data.html#link4, last seen on 20/10/2020.
[7] J. Pokorný, K. Saeed & V. Snášel, *How to Store and Process Big Data: Are Today's Databases Sufficient?* International Federation for Information Processing, 5, 5 (2014), available at https://hal.inria.fr/hal-01405547/document, last seen 20/10/2020.

tool for global markets, it's hampering the rights of consumers. Big Data is rather a loop which has no end to it. Technology is the strongest weapon and data is the propellant to it. Since its difficult to trace the source or track the flow of data over the internet and other databases, misuse of it is bound to happen. Hence, with the improvement and dependence on Big Data, additional responsibilities have to be borne by the collector.

II. CHANNELS AND ULTERIOR EFFECTS OF BIG DATA VIS-À-VIS PRIVACY AND CONSENT

Big Data is an excellent tool which facilitates in pooling gigantic amount of information. Any technology in itself does not provide for a diversion from its purpose, rather myriad channels are adopted by people using such a kind of technology for their personal gains and losses.

Privacy for a person is the space which must be ultimately untouched, but is also the most abused right. Once the personal data is collected, it is shared and reshared, sold and re-sold to an extent that it no longer remains 'personal' and 'private'.

Data brokers are companies that aggregate information about consumers from different sources, then license or sell that information to other organizations.[8] Data brokers hoover up personal identifiable information – in which specific information distinguishers can be traced or attributed to an individual's identity. The more data obtained, the more granular a profile of an individual can be.[9]

To begin with, by buying or licensing data or scraping public records, third-party data companies can assemble thousands of attributes each, for billions of people. For decades, companies could buy up lists of magazines subscribers to build targeted advertising audiences.[10] The information most

[8] M. Wlosik, *What is a Data Broker and how does it work?,* Clear Code, available at https://clearcode.cc/blog/what-is-data-broker/#what-are-data-brokers?, last seen on 12/12/2020.

[9] D. Leong & T. Yi-Ling, *Data Brokers: A Weak Link in National Security*, The Diplomat (21/08/2020), available at https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/, last seen on 24/10/2020.

[10] S. Melendez & A. Pasternack, *Here are the data brokers quietly buying and selling your personal information*, Fast Company, available at https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information, last seen on 24/10/2020.

closely related to one's spending habits is usually the most valuable to data brokers. Some of the data businesses are looking for, and can easily obtain information on household income, size and the ages of the members of your family, investment propensity, frequency by which you make large purchases, age and gender, educational status, general interests, and how you tend to spend your money on, like major life changes such as marriage, the birth of a baby, or retirement.[11] These profiles are then licensed or sold to companies to inform their business operations in marketing or in advertising products and services to customers. Companies utilize data-driven marketing to deliver more targeted and profiled advertising to consumers.[12]

Third party threats are a growing concerning too. Banks should also make sure they are only working with third parties that have appropriate security infrastructure in place, to mitigate the chance of any data being stolen.[13] It is important to gain access to third party environments or applications that can access the primary parties' database.

Apart from this, data tracking is another concern. Once the data of consumers is collected, the data analysts work towards analyzing that piece of information and try to reproduce as many pieces of information as possible. For the process to continue, they track all of our online behavior, with the available information. Thus, a simple mechanism with complex procedures to track the market behavior of consumers, opens a door for another business.

Seeing from the perspective of business, this seems a threat to the birth right of every individual. But from a wider perspective, such personal information of individuals can be a threat to the nation's security too. Data protection has become an important objective of countries around the globe. The need to keep a tab on data flow is necessary. Since such data

[11] *What is Big Data analytics and what does it mean to the consumers?,* Money Crashers, available at https://www.moneycrashers.com/big-data-analytics-consumers/, last seen on 24/10/2020.
[12] Supra 6.
[13] K. Flinders, *Digital bank customer data breached through third party*, Computer Weekly (28/07/2020), available at https://www.computerweekly.com/news/252486767/Digital-bank-customer-data-breached-through-third-party, last seen on 25/10/2020.

obtained is exploited commercially in the later stages, the ultimate source to obtain it is unknown.

Most legacy systems can't cope with the growing workload. Trying to collect, store, and analyze the required amounts of data using an outdated infrastructure can put the stability of your entire system at risk. With so many different kinds of data and its total volume, it's no surprise that businesses struggle to cope with it. This becomes even more obvious when trying to separate the valuable data from the useless.[14]

Such data can be accessed by anybody. Some countries are trying to ensure that the geolocation information is stored locally for national security considerations since having access to important information internationally can make a difference in a conflict. But companies in countries with rigid data residency and access requirements will acquire less crucial information in times of emergency because they are not trusted by business partners and governments abroad. Some countries seem to believe that crucial information will be safer at home. But, countries with isolated or outdated technology are less able to protect locally stored data against foreign military and criminal threats.[15] One of the chief concerns which the formulation of a data protection regime has to take into account is that while the web is a source of lawful activity-both personal and commercial, concerns of national security intervene since the seamless structure of the web can be exploited by terrorists to wreak havoc and destruction on civilized societies.[16] The modern warfare would happen not with weapons and missiles, but with this data, while sitting behind the computer.

Apart from diversion of right to privacy, Big Data can become a personal threat to the consumer himself and can expose him to various cybercrimes. Big Data companies like Amazon heavily rely on distributed computing, which typically involves data centers geographically dispersed across the

[14] A. Chalimov, *Big Data in the banking industry: the main challenges and use cases*, Eastern Peak (10/01/2019), available at https://easternpeak.com/blog/big-data-in-the-banking-industry-the-main-challenges-and-use-cases/, last seen on 25/10/2020.
[15] *How data residency laws can harm privacy, commerce and innovation - and do little for national security*, World Economic Forum (09/06/2020), available at https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/, last seen on 25/10/2020.
[16] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

whole world. Amazon divides its global operations into twelve regions each containing multiple data centers and being potentially subject to both physical attacks and persistent cyberattacks against the tens of thousands of individual servers housed inside.[17]

The consumer might have consented to the terms and conditions, but whether it is a consent to put their data on sale is the question. An informed consent, in present situation is not 'informed' *prima facie*. Definitely, the consumers would not have consented for the above ulterior effects through Big Data analytics. Consent, should be expressed restrictively in a sensitive matter, rather than assuming the broadest interpretation. Informed Consent must be prevented from being misused as a defense by the market.

As big is the Big Data, so are its consequences. If the size of the data is big enough, precise personal information can be obtained. A healthy market system must be a one, which benefits itself with the benefit of all. At the same time, such a system cannot be maintained as it operates in an *in vivo* environment and is susceptible to changes, fashions and attitudes of humans. But such susceptibility must not expose the consumer, the main component of this system, to face adverse consequences. A relation of harmony and trust must be established in every operation of business. Profits and other gains must not cost an individual's privacy.

III. 'CONSUMER' - THE DYNAMICALLY CHANGING STATUS UNDER PRIVATE FUNCTIONARIES

The meaning of consumer must be analyzed considering the fact that the market too has changed its way of business. Plainly, a consumer is a person who buys goods and services in exchange for consideration. But the process of buying itself has become advanced and complex, with the advent of technology. E-commerce has opened the gate for the market to move faster. Diversity is an attributed factor to it.

[17] J. Ryoo, *Big data security problems threaten consumers' privacy*, The Conversation (23/03/2016), available at https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798, last seen on 25/10/2020.

Institutions which analyze electronic data can build a user's behavior profile which contains attributes like the user's browsing history, transaction history, sex, profession, earnings, age and other demographics. The user behavior profile can be used to provide a more accurate and specialized service.[18] In such as system, the concept of consumerism is no longer archaic. Thus, it is essential to clarify the status and meaning of a consumer with respect to various institutions, impact of Big Data on them and misuse of consent.

1. Electronic Banking or E- banking

A customer is the one who uses a financial institution's services for their benefit. Significant progression in Information Technology has created a universal revolution in financial institutions. Substantial changes in financial systems are initiated by globalization and financial liberalization.[19]

Big Data analytics is now being implemented across various spheres of banking sector, and is helping them deliver better services to their customers, both internal and external, along with also helping them improve on their active and passive security systems. Banks today use spending patterns of their customers, perform consumer behavior based analysis on their channel usage, consumption patterns and segment consumers, to identify potential customers for selling financial products.[20] By integrating and analyzing data, banks have an opportunity to get a more accurate view on their customer's preferences.[21] The latest progress in

---

[18] S. Sharma, *A study on data mining horizons*, 2 International Journal of Recent Trends in Engineering & Research, 322, 322 (2016), available at https://www.ijrter.com/papers/volume-2/issue-4/a-study-on-data-mining-horizons.pdf, last seen on 26/10/2020.

[19] R.A. Aziz, R.E. Badrawy & M.I. Hussien, *ATM, internet banking and mobile banking services in a digital environment: The Egyptian banking industry*, 90 International Journal of Computer Applications, 45, 45 (2014), available at https://www.researchgate.net/publication/327534978_ATM_Internet_Banking_and_Mobile_Banking_Services_in_a_Digital_Environment_The_Egyptian_Banking_Industry, last seen on 26/10/2020.

[20] U. Srivastava & S. Gopalkrishnan, *Impact of Big Data Analytics on Banking Sector: Learning for Indian Banks*, Science Direct, available at https://www.sciencedirect.com/science/article/pii/S1877050915005992#:~:text=Banks%20reap%20the%20most%20benefits,for%20themselves%20and%20their%20customers.&text=Customer%20Segmentation%20and%20Profiling,profiling%20to%20increase%20hit%20rate, last seen on 27/10/2020.

[21] N. Sun, J.G. Morris, J. Xu, X. Zhu & M. Xie, *iCARE: A framework for big data-based banking customer analytics*, 58 International Business Machines Corporation Journal,

Information Technology makes it possible to integrate and analyze millions of records which include personal data.[22]

Increased competition and fast paced technological innovation in financial markets have forced banks to invest in online banking systems and other financial delivery channels to retain competitive advantage, revitalize customer relationship management and give customers the opportunity to perform real time financial actions easily and independent of time and place.[23] Perceived risk is one of the main inhibitors for internet banking usage and can be described as a customer's opinion of uncertainty and probable negative consequences of making use of internet banking.[24] United States digital bank Dave has reported a breach of customer data after hackers gained access through third-party technology supplier.[25] Passwords, as well as personal user information such as names, e-mails, birth dates, addresses and phone numbers, were included.[26]

In order to keep up the pace, E-banking websites often fail to protect the obtained data of consumers. Neither the consumer's consent is taken while pooling their data nor it is duly protected. Most of the activities occur through online transaction. Consumers are bound to update their bank details and other personal information to do so. Thus, such data is susceptible to be mined by the institution itself. Such Big Data pool is also

---

Research and Development, 1, 1 (2014), available at https://www.semanticscholar.org/paper/iCARE%3A-A-framework-for-big-data-based-banking-Sun-Morris/8e48fdca32b7b5bcb74cc5b3e6a2585b544c7cea, last seen on 27/10/2020.

[22] S.T. Ahmad, S. Haque & S.M.F. Tauhid*, A details study of data transformation for privacy preserving in data mining*, 5 International Journal of Scientific & Engineering Research, I, 2 (2014), available at https://www.ijser.org/paper/A-Details-Study-of-Data-Transformation-for-Privacy-Preserving.html, last seen on 28/10/2020.

[23] A.A. Shaikh & H. Karjaluoto, *Mobile banking services continuous usage-Case study of Finland*, 1 International Conference on System Sciences, 1497, 1497 (2016), available at https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNB7cjja/pdf, last seen on 28/10/2020.

[24] J.R.S. Fonseca, *E-banking culture: A comparison of EU 27 countries and Portuguese case in the EU 27 retail banking context*, 21 Journal of Retailing and Consumer Services, 708, 709 (2014), available at https://www.sciencedirect.com/science/article/abs/pii/S096969891400068X, last seen on 28/10/2020.

[25] A. Hrushka, *Dave security breach exposes 7.5M users' data,* Banking Drive (28/07/2020), available at https://www.bankingdive.com/news/dave-security-breach/582426/#:~:text=A%20security%20breach%20exposed%20the,Waydev%20was%20breached%2C%20Dave%20said, last seen on 12/12/2020.

[26] Supra 13.

exposed to various dangers, including hacking. The data sold thereupon exposes the consumers to cyber identity thefts, phishing, credit and debit card frauds and so on.

2. E- Education Facilities

Since education is a service and students enjoy it by paying at least minimal fees in extremities, they are the consumers. Educational Institutions are covered by the provisions of the Consumer Protection Act, 1986 ("**CPA, 1986"**).[27] If a student is aggrieved by the service/if an educational institution's service has a deficiency, a student can avail justice. Education sector has been streamlined to compete in the market. Various online education services are blooming rapidly. Students have access to online courses and distance education courses, provided online by various educational institutions. Though the service is delivered through many ways, the service intended to be delivered remains the same. Thus, such online service providers use the cyber platform to dispense their services, and students provide their information along with other data during enrolment and registration process.

In many cases, while in college, students begin to prepare themselves, financially, for the rest of their lives. They apply for jobs, rent apartments, and purchase vehicles. Such endeavors require financial stability, therefore, having personal data stolen could be detrimental. Larger universities hold more faculty, student and alumni data, proving that the more records a university holds, the more likely they are to be breached.[28] Schools face high costs as a result of data breaches. A study by the Ponemon Institute shows that the average cost of a data breach is USD 141 per record, but in education it typically reaches USD 200 per record (and has been even higher, with the four-year price averaging USD 260).[29]

---

[27] The Consumer Protection Act, 1986.

[28] M. Samantha, *Data Breaches in Higher Education Institutions,* University of New Hampshire Scholar Repository*,* available at https://scholars.unh.edu/honors/400, last seen on 27/10/2020.

[29] R. Carr, *The Rise of Education Data Breaches*, Zettaset, available at https://www.zettaset.com/blog/education-data-breaches/, last seen on 27/10/2020.

Big Data can impact higher education practices, from attractive student experiences to improved academic programming, to more effective evidence-based decision making, and to strategic response to changing global trends, but has the potential to turn complex, often unstructured data into tortious information.[30] In addition, monetary variables such as high-income students, faculty salary, and median and average family income show significance. The more data elements a university protects, the less likely a breach will occur. This indicates that universities should not only be taking actions to secure privacy but also to ensure the most amount of data possible is suppressed.[31]

Online education start-up Edureka suffered a significant data leak that exposed sensitive personal information such as names, addresses, phone numbers of at least 2 million users. *"Given that Edureka provides professional-grade online courses to people, often in significant or powerful positions and with access to highly-sensitive information, the company's compromised server security could have been devastating to entire organizations such as universities, companies or government departments"* said a lead security researcher of that case.[32]

Escola Digital, a Brazil-based online learning platform, suffered a data leak that exposed over 75,000 private records (15MB) of students and teachers.[33] South Africa-based online learning platform MyTopDog lost over 800,000 students' personal records (40-50MB).[34] Okoo, a Kazakhstan-based online course portal, lost around 7,200 records (418MB) that held students' personally identifiable information and administrative data.[35] The U.S.-based online education platform Square Panda lost around 15,000 personal records (1MB) of parents and teachers.[36] S.-based virtual learning

[30] M. Hilbert, *Big Data for Development: From Information- to Knowledge Societies*, SSRN, available at http://ssrn.com/abstract=2205145, last seen on 27/10/2020.
[31] Supra 23.
[32] Salman SH, *Edureka's database breached, 2 million user records potentially at risk,* LiveMint, available at (30/09/2020) https://www.livemint.com/companies/start-ups/edureka-s-database-breached-2-million-user-records-potentially-at-risk-11601450797202.html, last seen on 27/10/2020.
[33] C. Williams, *Data leaks in Online education: Almost 1 million data exposed,* WizCase (02/10/2020), available at https://www.wizcase.com/blog/educational-breaches-research/, last seen on 16/12/2020.
[34] Ibid.
[35] Ibid.
[36] Ibid.

platform Playground Sessions' data leak exposed nearly 4,100 user records (1.2MB).[37]

Presently, most of the universities are not equipped with a strong and protected system to protect such data. Considering the other institutions, mining data from websites and other databases of educational institutions is an easier option. Generally, such websites give public access for viewing the functioning of the institutions, their alumni profile, portfolio of the teaching faculty and so on. Anyone can easily access data through this means. Institutions provide student grant facilities, wherein data regarding their profile and other information shall be stored. If leaked, it can be used for many ulterior motives, or even sold to companies by data brokers and hackers. Consent of students for such dangers is a silent factor.

3. Medical Institutions and Tele-Medication

Telemedicine is a modern and a scientific approach in health care system with the use of telecommunication and information technologies to provide clinical health care at a distance. Telemedicine also referred to as telehealth allows health care professionals to evaluate, diagnose and treat patients in remote locations using telecommunication.[38] Telenursing is defined as the use of telecommunication technology to deliver nursing services to client at a distance.[39] Nurses engaged in telenursing practice continue to assess, plan, intervene, and evaluate the outcomes of nursing care, but they do so using technologies such as the internet, computers, telephones, digital assessment tools, and telemonitoring equipment.[40] Bearing in mind that health services now provided via tele-technologies

[37] *E-Learning Platforms Continue to Suffer Data Breaches; 1 Mn Records Exposed*, Cisomag (20/07/2020), available at https://cisomag.eccouncil.org/data-breaches-on-e-learning-platforms/, last seen on 27/10/2020.

[38] S.K. Passyavula, *Telemedicine, telenursing & tele education -A revolution multi-innovation in current nursing scenario*, 2(5) International Journal of Medical and Health Research, 31, 32 (2016), available at http://www.medicalsciencejournal.com/archives/2016/vol2/issue5/2-5-23, last seen 28/10/2020.

[39] J. J. Fitzpatrick & M. Kazer, *Encylopedia of Nursing Research*, (3rd ed., 2011).

[40] Peck, Amy RN, *Changing the Face of Standard Nursing Practice Through Telehealth and Telenursing,* 29(4), Nurse Administration Quarterly, 339, 340 (2005), available at https://journals.lww.com/naqjournal/Citation/2005/10000/Changing_the_Face_of_Standard_Nursing_Practice.8.aspx, last seen on 16/12/2020.

have expanded, the term telehealth is used to capture the breadth of services.[41]

A patient is a consumer since he enjoys the service of the doctors and medical fraternity for the fees paid. Though health care is removed from the meaning of service under Section 2(42) of the Consumer Protection Act, 2019 (**"CPA"**),[42] it contains the phrase "*includes, but not limited to"* and the same is an inclusive clause. It directly points out to the fact that 'healthcare' can still be included and interpreted under Section 2(42) of the CPA.[43] Since this is discharged via online nowadays, concerns regarding privacy policy and data mining come into issue. Thus, a patient is still a consumer and implied consent of his to enjoy services online should not be mistaken as a nod to compromise with privacy.

The personal data of 2,373,764 patients was left exposed online after Hova Health, a telemedicine company based in Mexico, misconfigured a MongoDB database. The database contained patient names, personal ID codes for Mexican citizens and residents, insurance policy numbers and expiration dates, dates of birth, and addresses. There also were flags noting migrant status or disabilities.[44] Misconfiguration issues are far too common for the healthcare sector, which already is being pummeled by cyberattacks. One wrong click and tens of thousands to millions of patient records can be breached.[45] Telehealth start-up Babylon Health just suffered a data breach that mistakenly sent videos of patients' private consultations with

---

[41] L. Schlachta-Fairchild, V. Elfrink & A. Deickman, *Patient Safety, Telenursing, and Telehealth*., In. Patient Safety and Quality: An Evidence-Based Handbook for Nurses, (Hughes RG, Rockville (MD): Agency for Healthcare Research and Quality (US); 2008 Apr. Chapter 4). available at https://www.ncbi.nlm.nih.gov/books/NBK2687/, last seen on 28/10/2020.

[42] The Consumer Protection Act, 2019.

[43] S. Paliwal & G.S. Gaur , *Exclusion Of 'Healthcare' From The Definition Of 'Service': A Delusional Relief For Medical Professionals*, Mondaq (11/08/2020), available at https://www.mondaq.com/india/healthcare/975294/exclusion-of-healthcare39-from-the-definition-of-service39-a-delusional-relief-for-medical-professionals, last seen on 28/10/2020.

[44] J. Davis, *Telemedicine vendor breaches the data of 2.4 million patients in Mexico*, Healthcare IT News (07/08/2018), available at https://www.healthcareitnews.com/news/telemedicine-vendor-breaches-data-24-million-patients-mexico, last seen on 02/11/2020.

[45] Ibid.

doctors to other patients.[46] The breach was brought to Babylon Health's attention after a patient tweeted a screenshot, showing he had access to dozens of other people's consultation videos.[47] As the numbers of new and innovative technologies emerge, researchers and developers must remember the security of patient information, regardless of how it is transmitted.[48]

4. E- Commerce

Modern consumer's activity of shopping necessities and luxuries have been operated online increasingly. With discounts and gift vouchers available throughout the year, consumer's first choice is online shopping, through E- commerce websites.

The *modus operandi* is that a consumer has to create an account, view and order a product and choose one among various payment methods. Most of the time, consumers pay online via various payment methods. Phone numbers and E-Mail IDs are collected. Thus, such platforms keep a track on category of items a consumer constantly views and sends messages regarding current deals. This proves that e-commerce websites keep track of our information and preferences via Big Data technology. But ensuring the safety of such information is necessary. As the consumers are reaping benefits from online services as such, they are getting exposed to numerous cyber threats, where personal data is sold for a price.

User data from online grocery platform BigBasket is for sale in an online cybercrime market. The data comprised names, E-Mail IDs, password hashes, PINs, mobile numbers, addresses, dates of birth, locations, and IP addresses. Part of a database containing the personal information of

[46] L. Kelion, *Babylon App admits GP app suffered a data breach,* BBC News (09/06/2020), available at https://www.bbc.com/news/technology-52986629, last seen on 16/12/2020.
[47] A. Holmes, *A telemedicine app accidentally leaked videos of people's medical consultations to other patients*, Business Insider (10/06/2020), available at https://www.businessinsider.in/tech/news/a-telemedicine-app-accidentally-leaked-videos-of-peoples-medical-consultations-to-other-patients/articleshow/76307541.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, last seen on 02/11/2020.
[48] Supra 20.

close to 20 million users was available with a price tag of INR 3 million (USD 40,000).[49]

Thus, one point to conclude from the above information is that the consumers are not the main facet, but a part and parcel of the global profit system. A consumer's consent should be taken, and such consent shall not be implied as a green signal to use his rights and personal space as a raw material. When a website requests for personal information, it is a bounden duty to protect it.

IV. E-GOVERNANCE, BIG DATA, CONSUMER CONSENT AND PRIVACY

Governments in any given country will have a wide-ranging purpose for amassing data, which reflects to be differing from that of businesses to a considerable extent. The key intention of businesses to collect data is to achieve profits and keep the customers happy and satisfied. But the distinctive object of the government includes maintaining domestic peace and tranquility, achieve sustainable development, secure citizen's basic rights, promote general welfare and economic growth.[50] In all, the

[49] S. Gosh, *Apparent data breach at BigBasket reveals the need for e-commerce players to bolster cybersecurity measures*, CSO India, available at https://www.csoonline.com/article/3596873/apparent-data-breach-at-bigbasket-reveals-the-need-for-e-commerce-players-to-bolster-cybersecurity.html, last seen at 10/01/2021; *BIGBASKET, India's leading online supermarket shopping allegedly breached personal details of over 20 million people sold in Dark web*, available at https://cybleinc.com/2020/11/07/bigbasket-indias-leading-online-supermarket-shopping-allegedly-breached-personal-details-of-over-20-million-people-sold-in-darkweb/?__cf_chl_captcha_tk__=5711add3a5e2c69e10165212b8435433b0a5dfce-1610302048-0-ARSairp5Z40FiaO_3gb_UYsO7Izw6xBYq7ASBXimg5-kpJ126nWEUXA_xje9_uykMuX-Cx3o6nHqSrj52IUar4Lr3Blo0NBgv-Kj_w8Fe0MYw3Z4KiYgFfjzdV2aptwBGZrSuErqjB54Fo3urMj9hh2lpB9TjZEN1ZgRR2tdSp1P3CWLt7oGP3XwD0YFsq9jhshbNkpeDZ2NHXVTflDcTAaB-F8wRk2DELowyP39RzK3VwyvJPTPLFD2e9hLtXj978Wm5fEL0CDR6lIJ8h2q-syu4flN6phetgGb7wNhV0CLXQnPTgjkyOzzLQHS8JFTlIZPnDHxYeeAyomMyXXJw0EO6YlO_BDVTX01yQlPIuEg7X6nPq0m0yTKeYsH_rtiUi_rirviO1CGvOHkhX-DTglErxP9J_7WMpSaVDNCHTwXo4ZUqTuv59ZXwlNHadD6Y-qXifdm8GC2FdM0Nm21fxrsHwjJxEZp1-uIKCDlqMh9Mk6UkFliqJH6nIBpe9FDdP8jYAPslvuMWePkYk2o0aQMRI8i5nHIwyQrkOrZJhICxFxb-G7z2EWJZw5tf3grM9NXxP4M62mcFIaXrwQXcrnoTrUrV4qZHWMVem7huK_hPbkGk5u6nW3MZ0J0VD_7b6FwGV7zxCG-HuDbFazko64UptU49LeUnwV--gxVoqiP_uxhLetjSvaX5xiJQeN7BWwuHcr5SQXPj_OpM9z-S6o, last seen on 10/01/2021.

[50] G. Kim, S. Trimi & J. Chung, *Big-Data Applications in the Government Sector*, Communications of the ACM, March 2014, Vol. 57 No. 3, Pages 78-85, available at https://cacm.acm.org/magazines/2014/3/172509-big-data-applications-in-the-government-sector/fulltext#R18, last seen on 02/11/2020.

government's target revolves around the citizens and their well-being. These targets are achieved by rendering services to the citizens by different government departments. The conventional mode of performing these functions is through offline mode wherein the citizens visit respective offices where the desired services are rendered.

A significant dilemma of whether government services can be held liable for deficiency of service under the CPA, 1986 has been elucidated in various cases like *Shamsher Khan* v. *Rajasthan State Electricity Board*[51] where the applicant had applied to Electricity Board for electricity connection for a flour mill but there was a delay in releasing the connection. He filed a complaint for deficiency in service and was held a consumer under the Act. Thus, a statutory corporation which is a government body was held liable for deficiency in service.

Similarly, in *Shri Prabhakar Vyankoba Aadone* v. *Superintendent, Civil Court*[52] ***("Aadone")***, the National Commission held that an applicant for certified copy of a judicial order, who deposits a fee for obtaining such copy is a 'Consumer' within the meaning of the CPA, 1986 and the processing of such application and the preparation and delivery of the copy in consideration of the copying charges/fee by the concerned staff attached to the court would be a service within the meaning of the Act. This view was further upheld by the Commission in *Dr. Chandrakant Vitthal Sawant* v. *L. R. Pilankar Inspector of Land Records*[53] ***("Vitthal")***, in which it was held that the petitioner who had approached the respondent authority for carrying the measurement of the land in question by paying the requisite fees is a consumer and the functions of the respondent would constitute service.

E-Governance or electronic governance can be defined as the application of information and communication technology (**"ICT"**) for providing government services, exchange of information, transactions, integration of previously existing services and information portals[54]. The perspective of

[51] Shamsher Khan v. Rajasthan State Electricity Board, (1993) II CPR 6 (Raj.).
[52] Shri Prabhakar Vyankoba Aadone v. Superintendent, Civil Court, 1986 2004 Consumer 7211 (NS).
[53] Dr. Chandrakant Vitthal Sawant v. L. R. Pilankar Inspector of Land Records, 2013 SCC Online NCDRC 642
[54] F. Barrister & R. Conolly, *Defining e-Governance*, e-Service Journal 3, 4 (2012).

e-governance is *"the use of the technologies that both help to govern and have to be governed"*.[55] The central goal of e-governance is to reach the beneficiary and to ensure that their service needs are met. With the surge to associate digitalization with the ideology of welfare state, the need for e-governance transpired. Every Ministry, government departments, agencies could now function, store and update records, attend to the needs of the citizens through their websites or mobile applications.

Through Section 2(7) of the CPA the government widened the definition of 'consumer' by inserting explanation (b) which states that, the expressions 'buys any goods' and 'hires or avails any services' includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing.[56] The central government has been allowed to take steps and draft guidelines to discourage discriminatory e-commerce activities in order to protect customers' privileges and interests. The CPA, 1986 did not specifically include e-commerce transactions, and this lacuna has been addressed by the new Act. Now, a new dilemma arises: whether the citizens availing the services of e-governance are 'consumers' and whether services provided through e-governance constitute 'service' under the CPA. And if it does, will the government be liable for misuse of personal data or violation of privacy of the citizens stored in the Big Data bank.

In its website, the Ministry of Consumer Affairs has included e-governance division where it declares its vision: *"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man"*[57]

It further declares: *"The Government of India is focused on using technology to the maximum possible extent to give fillip to effective and efficient governance. To achieve the objective of providing consumer-friendly services, the department has digitized its various*

[55] P. Rossel & M. Finger*, Conceptualizing e-Governance Management* (2007): 399–407.
[56] Explanation (b), S. 2(7), The Consumer Protection Act, 2019.
[57] Department of Consumer Affairs, *E-governance,* Ministry of Consumer Affairs, Food and Public Distribution, available at https://consumeraffairs.nic.in/organisation-and-units/division/e-governance, last seen on 08/11/2020.

functions." Thus, relying on the declaration, services provided through e-governance to the citizens makes them consumers.

The goal of government-to-citizen (**"G2C"**) e-governance is to offer a variety of ICT services to citizens in an efficient and economical manner and to strengthen the relationship between government and citizens using technology.[58] Mundane services such as name or address changes, applying for services or grants, or transferring existing services are more convenient and no longer have to be done in person.[59]

The citizens avail these e-services through the respective department's website/portal by paying the prescribed fee. As held in *Aadone* and *Vitthal,* the charges paid while applying for the services is consideration fee and the function of the office constitutes service. Thus, a consumer and service provider relationship are established between the citizen and the government when consideration fee is paid for the service.

Through e-governance platforms, the government is functioning at an improved efficiency, reliability and pace. With this development, the gravity of application of Big Data was realized. Until the recent years, utilization of Big Data by the government was spotted only for keeping tabs of huge data produced in the course of functioning of various governmental ministries, departments, agencies, intelligence services, etc. But with the foundation of e-governance, the velocity at which data is produced is enormous. Technology relating to Big Data is developed to an extent where a humungous amount of data produced like in the Unique Identity Project, Digital India program, etc. can be collected, stored and analyzed for any desired outcome.

With the view to provide value-added services to citizens through e-governance, the government has failed to address the shortcomings of digitalization on the privacy of citizens. In fact, the privacy issues dominate over the benefits of e-governance in every digital platform that the government has introduced.

---

[58] *E- governance*, Wikipedia, available at https://en.wikipedia.org/wiki/E-governance, last seen on 16/12/2020.

[59] W. Miller & J. Walling, (2013), *Government in the twenty-first century: New Avenues of Study*, *Taking Sides*. New York, NY: McGraw Hill.

One such case, is of Aadhaar, which is the world's largest biometric identity platform. With an enrolment of over 1 billion registrants,[60] Aadhaar exhibits data challenges like data volume, variety and velocity which are the characteristics of Big Data. This digital identity system facilitates both the government and private sector, the precious enormous data of residents. It has become the *de-facto* identity document accepted by all service providers like private banks, schools, hospitals, telecom operators to buy SIM cards, medical insurance or any other utility services. While availing any government service, citizens are required to provide their Aadhaar number which gets uploaded in their records and further on Big Data bank. The biometric identifiers which are considered to be a boon can pose a threat of data breaches and misuse of personal data which may lead to violation of privacy and human rights of the citizens.

Linking of Aadhaar to various accounts and documents like bank account, Permanent Account Number (**"PAN"**) card, social security schemes, mobile SIM cards, pension account, Liquefied Petroleum Gas (**"LPG**") connection, driving license possessed by the citizens has been made mandatory. Once linked with Aadhaar, all the data connected with these accounts and documents get stored in the Big Data bank. Any alteration made to them will get updated in the Big Data storage. Every document and account possessed by the citizens contain sensitive information of their lives, religion, sexual orientation, residential address, etc. Big Data technologies can potentially be used to discriminate against vulnerable groups and manipulate information. Following are the features of Unique Identity Project, Aadhaar which compromises the privacy of the citizens when the documents are linked:

1. The Central Identities Data Repository

Aadhaar database containing all Aadhaar numbers, demographic and biometric information is stored in Central Identities Data Repository

[60] *AADHAAR Dashboard*, Unique Identification Authority of India, available at https://uidai.gov.in/aadhaar_dashboard/index.php, last seen on 16/12/2020.

(**"CIDR"**) which is a centralized database.[61] Both username (Aadhaar number) and the password (biometric information) being stored in this same database has made the citizens' personal data vulnerable to misuse. Further, the Aadhaar database is stored in about 7000 servers in two data centers located at Bangalore, Karnataka and Manesar, Haryana.[62] If any of the two data centers is compromised, there is no certain answer as to the consequence on the highly sensitive and personal data of millions of residents.

2. Ginger Platform

Service providers that adopt the Aadhaar number of the residents in their service delivery database i.e., seeding, will have to move their existing databases onto the Ginger platform, which then organizes the present and incoming data in the database by individual Aadhaar numbers. Once organized, anyone having access to the 'control' end of the Ginger platform can access all data associated to an Aadhaar number.[63] It further facilitates profiling of individuals through convergence of databases on this platform which can then be accessed by the Unique Identification Authority of India (**"UIDAI"**). The seeded data of the individuals containing inherent psychological and behavioral characteristics can be utilized by the Government or anyone with the access. Thus, the ginger platform lacks protection on the personal and sensitive information of the citizens.

3. Freedom of Speech and Expression

Every citizen's data will be collected and stored by different agencies throughout his lifecycle. The data begins from birth certificate, education, scholarships, driver's license, passport, employment, taxes, marriage

---

[61] Amber Sinha, *The Unique Identity Project, Big Data in Governance in India: Case Studies, The Centre for Internet and Society, India*, available at https://cis-india.org/internet-governance/files/big-data-compilation.pdf, last seen on 16/12/2020.

[62] *Aadhaar-enabled DBT savings estimated over Rs 90,000 crore*, The Times of India (11/07/2018), available at https://timesofindia.indiatimes.com/business/india-business/aadhaar-enabled-dbt-savings-estimated-over-rs-90000-crore/articleshow/64949162.cms, last seen on 05/11/2020.

[63] E. Hickok, S. Chattapadhyay & S. Abraham, *Big Data in Governance in India: Case Studies,* The Centre for Internet and Society, India, available at https://cis-india.org/internet-governance/files/big-data-compilation.pdf, last seen on 08/11/2020.

certificate, banking, insurance, land records, court records, pension to the death certificate. It is an individual's cradle to grave profiling which enables greater surveillance and impedes anonymity. This will have an adverse impact on a citizen's freedom of speech and expression.

Since there is no detailed privacy framework, therefore there are possibilities that the Authority may use Aadhaar Card data against citizens. For example, during a protest, law enforcement agencies can record the videos of protesters, scan the iris data, and easily access information about protesters. Access to sensitive data of this nature gives unfair advantage to repressive governments and protesters are vulnerable to threats.[64]

4. Data Protection Regulation

The government agencies and third parties, in the absence of specific data protection regulation and privacy legislations, can access and share data among them. A consumers' life can be made miserable at every step when data can be shared with secondary motives. Absence of specific regulation hinders human rights and freedoms of the consumers, while the technology sees new developments. With an aim to introduce a specific regulation, the Personal Data Protection Bill, 2019 (**"PDP"**) was drafted to protect the personal data of the individuals and prevent any form of misuse. But with provisions which empowers the government to collect and access personal data,[65] the Bill defeats its own purpose of safeguarding the privacy of the citizens.

Citizens while availing services from the government through offline or online mode become consumers and provide their utmost sensitive personal data to the government departments. Any breach of data and violation of citizens' privacy is equal to violation of rights and interests of the consumers.

[64] B. Halder, *Privacy in India in the age of Big Data*, APC, available at https://www.apc.org/sites/default/files/Privacy-in-India-in-the-Age-of-Big-Data.pdf, last seen on 09/11/2020.
[65] S. 98, Personal Data Protection Bill, 2019 (pending).

V. CURRENT LEGISLATIVE ACTIONS AND JUDICIAL OPINION ON BIG DATA

Big Data's advent in India markets and its influence on administration can be seen a decade later, compared to other developed countries. When other countries have backed up with a series of streamlined policies and regulations, India is still on its way to pass an effective, holistic and inclusive policy. The concept of Big Data and the importance of protecting information privacy was discussed for the first in *K. Puttaswamy* v. *Union of India.*[66]

The judgement vividly explained concerns regarding the nature of Big Data, i.e., these data sets are capable of being searched, they have linkages with other data sets, and are marked by their exhaustive scope and the permanency of collection. Also, it rightly opined that the challenge which is posed by Big Data mainly arises from State and non-State entities.

Emphasis was laid on the fact that the balance between data regulation and individual privacy raises complex issues requiring delicate balances to be drawn between the legitimate concerns of the State on one hand and individual interest in the protection of privacy on the other. Reference was made to the European data protection regime on the centrality of consent. It was held that a mere consent from the users is not a validation to exploit the data obtained and reuse it. The judgement also laid down that formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State.

With digital and technological revolution, India has welcomed multiple players into its market without establishing a formal regulation on data protection. Data revolution has reached to an extent where data mining has no legitimate boundary. The absence of specific regulation adds onto the inaccurate manipulation of data sharing, side-lining the most valuable aspect of the consumers i.e., privacy.

[66] Supra 16.

1. Information Technology (Amendment) Act, 2008

Certain aspects of data protection are covered under the Information Technology Act of 2000 (**"IT Act"**) and the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules of 2011 (**"Data Protection Rules"**). But the scope of these statutes is diminishing with enhanced technological developments.

The rules limit itself to companies, including firms, sole proprietorships, and associations of individuals engaged in commercial/professional activities (collectively, the 'body corporate')[67] and does not include government bodies and individuals engaged in data processing. This has contributed to validation of mass surveillance, profiling of individuals and misuse of citizen's personal data by the government which has an exponential impact on the individual's independence. Section 43A, which requires the *maintenance of reasonable security practices and procedures by bodies corporate that possess, deal or handle any sensitive personal data or information and* provides for *compensation for failure to protect such data*[68] and Section 72A, which penalizes intentional personal data breach were incorporated.[69] The amendment however did not provide for distinct definitions of personal data or sensitive personal data. Section 43A provided that 'sensitive personal data or information' would mean such personal information as would be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Rule 3 of the Data Protection Rules provides an exhaustive list of eight types of personal data as sensitive personal data: i) password; ii) financial information such as bank account or credit card or debit card or other payment instrument details; iii) physical, physiological and mental health condition; iv) sexual orientation; v) medical records and history; vi) biometric information; vii) any detail relating to the above clauses as provided to body corporate for providing service; viii) any of the

[67] Explanation (i), S. 43A, Information Technology Act, 2000.
[68] S. 43A, Information Technology Act, 2000.
[69] S. 72A, Information Technology Act, 2000.

information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.[70]

The limited scope of 'sensitive personal data or information' is an additional limitation. As technology like the IoT, facilitates ubiquitous data collection, other sensitive personal information such as location, habits, and activity among others should be encompassed by the purview of these Rules.[71]

Rule 6 provides for disclosure of sensitive personal data with prior permission.[72] There is ambiguity regarding regulation for disclosure of non-sensitive personal data. Being in an era of IoT, where sensitive personal data can be derived out of any available non-sensitive personal data, the purpose of this rule seems futile.

2. Personal Data Protection Bill, 2019

With the profound necessity to regulate how personal data should be processed and stored and the procedure on who can and how to access the personal data of the consumers/citizens, the PDP was introduced in the Parliament on December 11, 2019. A framework on people's rights on their personal data is also provided in the Bill.

'Consent' is the paramount prerequisite that must be achieved before accessing any kind of data of the citizens. The Bill does not provide a clear definition of 'consent' or 'explicit consent'. The Bill furnishes a diverse circumstance where consent is not required for data processing of individuals. When there is strict necessity for the State, even the explicit consent required to access sensitive personal data can be overlooked. Consent is the only exception which when taken the citizen's right to privacy claim can be defended against. The Bill confers unrestricted power

[70] Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[71] S. Basu & R. Malik, *Big Data: A Challenge to Data Protection?,* India Law Journal, available at https://indialawjournal.org/big_data_a_challenge_to_data_protection.php, last seen on 10/11/2020.
[72] Rule 6, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

on the state to access individual data which goes against the spirits of landmark 'right to privacy' ruling of the Supreme Court of India.[73]

The application of the Bill extends to the (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.[74] For the first time, the government is regulated under a bill with respect to data processing. But the main concern is that Section 98 of the Bill gives power to the central government to issue directions in certain circumstances to exempt any governmental agency from complying with the provisions of the Bill.[75] Wherever the Central Government is satisfied that it is necessary in the interest of sovereignty and integrity of India, the security of the State, public order, friendly relations with foreign states, it can direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data.[76] Further, the Government can access the personal data in the interest of wide reasons provided in chapter 8 of the Bill. The exemptional power vested with the government is very broad, leaving scope of misuse and misinterpretation of the same.[77] Surveillance of the citizens can be done legally under the Bill which impacts their freedom of speech, expression and association. Thus, the provision negates the purpose of regulating data processing by the government.

Even though, the Bill's scope is remarkably outstretched, it is the minute details that undermines the main purpose of protecting the rights and interests of the citizens, which must not be overlooked. In fact, the

[73] R.V. Anuradha, *Why the Personal Data Protection Bill spells trouble for India's IT sector*, CNBC TV 18 (01/08/2018), available at https://www.cnbctv18.com/views/why-the-personal-data-protection-bill-spells-trouble-for-indias-it-sector-402301.htm, last seen on 11/11/2020.

[74] S. 2, Personal Data Protection Bill, 2019 (pending).

[75] S. 98, Personal Data Protection Bill, 2019 (pending).

[76] M. Mandavia, *Data Protection Bill: Centre has the power to exempt any government agency from application of act,* Economic Times Government (10/12/2019), available at https://government.economictimes.indiatimes.com/news/policy/data-protection-bill-centre-has-the-power-to-exempt-any-government-agency-from-application-of-act/72456626, last seen on 16/12/2020.

[77] S. Katarki, N. Viswanath , I. Chatterjee & R. Reddy, *The Personal Data Protection Bill, 2019: Key Changes And Analysis*, Mondaq (06/01/2020), available at https://www.mondaq.com/india/privacy-protection/880200/the-personal-data-protection-bill-2019-key-changes-and-analysis, last seen on 11/11/2020.

provisions under the Bill are not free from ambiguity which again provide unfettered powers to the state while defending its preposterous acts.

3. CPA and Consumer Protection (E-Commerce) Rules, 2020.

Through Section 2(7) of the CPA the government widened the definition of 'consumer' by inserting explanation (b) which states that, *"the expressions 'buys any goods' and 'hires or avails any services' includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing."*

Section 2(47) of the CPA provides the definition of 'unfair trade practice' which states that, "*a trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice.*" The Section further includes a set of practices which constitutes 'unfair trade practice'. Clause (ix) of sec. 2(47) states that, *"disclosing to other person any personal information given in confidence by the consumer unless such disclosure is made in accordance with the provisions of any law for the time being in force."*

Even though, the Act has made an effort to restrict the misuse of consumer's personal information for the purpose of any kind of trade practices, it fails to give clarity on the aspects of consent of the consumers and sensitivity of the information. Considering the flourishing e-commerce activities, personal data of the consumers like location, mobile number, etc., are the most primitive requirements to avail the e-commerce services. The current data protection law i.e., Data Protection Rules does not include such primitive information as sensitive, thus leaving scope for misuse of the same.

The Consumer Protection (E-Commerce) Rules, 2020 has not touched upon the protection of the data and personal information provided by the consumer, especially when that information is also being accessed out of the country. Absence of specific guidelines regarding personal data under the rules has resulted in ambiguity which affects the compliance of the provisions under Sec. 2(47) of the CPA.

VI. OBSERVATIONS AND SUGGESTIONS

1. Extent of Consent

A raising issue which needs to be addressed is to determine the extent of consent given by the consumers while availing E-services. A framework[78] was released by the Government of India under the department of Ministry of Electronics and Information Technology and Department of Science & Technology in 2012. The main theme of the framework was focused on the necessity for a combined regulation to manage consent issues of a consumer.

Electronic consent is the digital equivalent of a physical letter of permission given by the user which, when presented, allows the data provider to share information regarding the user with a data consumer, for a particular purpose. Electronic consent allows for data to be electronically and securely shared with service providers on an as-needed basis, while maintaining traceability, to ensure that the data trails can be audited in the future. 'Consent' under the PDP must be defined with precision. In order to address the wide scope of situations while getting the consent of the e-service consumers, a set of rules must be framed. Procedural guidelines for exceptional cases where the consent may not be taken must be strictly formulated.

Thus, the government, being procured with the status to manage the country through law can give the status of statutes to mere frameworks, making it mandatory for the companies and other functionaries to follow it. E-consent management must be regulated precisely, since these are the upcoming issues for a modern democracy and a developing country in cyber era.

2. Determining whether a User is a Consumer or not?

The foremost observation is that whether a user of social network websites, apps and messaging platform is a consumer or not. With the increasing

[78] *Electronic Consent Framework - Technology Specifications (Ver 1.1)*, Ministry of Electronics and Information Technology, available at http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf, last seen on 11/11/2020.

usage and dependence on such platforms, there is no single person who does not use those. According to Facebook, social media is its product and it enables us to connect with people who matter, wherever they are in the world.[79] A user can not be a consumer if he/she does not pay for a product or service. Anything for free does not entitle the user as a consumer. But most of the social network websites, apps and messaging platform make profits by selling personal data of its users and moreover, they offer their services or facilities for free. A user has to sign in and create an account, thus entitled to use the application. But there are numerous cases and allegations against such platforms for misusing the data of its users. For instance, Facebook is 'free', but we pay with our personal information. That information is then used to sell targeted advertisements- the primary way Facebook makes money.[80] In the case of e-governance services, the determining factors concerning when the citizens will come to be consumers need to be demarcated. The conundrum regarding what constitutes services irrespective of whether consideration fee is demanded or not for availing e-services must be meticulously specified. The personal information received from the citizens like Aadhaar number, PAN, etc., which in turn possesses sensitive personal information must be regarded as the payment for services provided by the government through e-services.

Thus, the users cannot pay their privacy in return of service they avail. Privacy is an immeasurable asset. These platforms act like middlemen alone. Once they collect and sell the data, their business is over. What happens to such data is unknown. Thus, for all the innocent users, the only way of justice is to ascertain or fix their status.

3. Regulation of Anonymized and Pseudonymized Data

Many websites and applications claim that the data they collect is anonymized. Companies and governments both routinely collect and use

[79] B. Gilbert, *Facebook just published a message for its users: No, you're not the product,* Business Insider (23/04/2018), available at https://www.businessinsider.in/tech/facebook-just-published-a-message-for-its-users-no-youre-not-the-product/articleshow/63887171.cms, last seen on 16/12/2020.
[80] Ibid.

our personal data. Data is 'sampled' and anonymized, which includes stripping the data of identifying characteristics like names and e-mail addresses, so that individuals cannot, in theory, be identified. After this process, the data's no longer subject to data protection regulations, so it can be freely used and sold to third parties like advertising companies and data brokers.[81] This whole process is called as de-identification of data.

But in reality, such data can be reidentified. One can never escape from the harsh realities of Big Data. Such data which can be reidentified is called as pseudonymized data. According to a class action lawsuit[82] levied against the social media giant in January 2014, Facebook raked in USD 2.7 billion in sales for helping create targeted ads for companies based on the information its members posted online. While Facebook says the allegations are a myth and promises that it doesn't share personal information and never will, the Facebook Statement of Rights and Responsibilities sings a slightly different tune: It states that Facebook can and will sell personal information – once it's been anonymized.[83]

In 2016, journalists re-identified politicians in an anonymized browsing history dataset of 3 million German citizens, uncovering their medical information and their sexual preferences. The Australian Department of Health publicly released de-identified medical records for 10% of the population only for researchers to re-identify them 6 weeks later.[84] Researchers were able to uniquely identify individuals in anonymized taxi

[81] Imperial College London, *Anonymizing personal data 'not enough to protect privacy,' shows new study,* ScienceDaily (23/07/2019), available at <www.sciencedaily.com/releases/2019/07/190723110523.htm>., last seen on 07/11/2020.

[82] Mathew Campbell and Michael Hurley v. Facebook, Inc, 17-16873 (9th Cir) (2017, U.S. Court of Appeals), available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1611&context=historical, last seen on 07/11/2020.

[83] J. Curtis, *What Are Big Data Analytics and What Does It Mean for Consumers?*, available at https://www.moneycrashers.com/big-data-analytics-consumers/, last seen on 06/11/2020.

[84] C. Culhane, B. I. P. Rubinstein & V. Teague, *Health data in an open world*, Cornell University (15/12/2017), Preprint available at https://arxiv.org/abs/1712.05627, last seen on 06/11/2020.

trajectories in New York City,[85] bike sharing trips in London,[86] and mobile phone and credit card datasets.[87]

Thus, the entire act is like a circle. It's a process where data is claimed to be de identified, but later reidentified to be used for profits. Anonymized data still carries potential to reveal personal information. Hence, modern tools can be developed which forbid companies and other institutions to re identify anonymized information for safety and security concerns of an individual. Also, stringent data regulation policies are necessary to regulate pseudonymized data, the functionaries who are allowed to use it and situations under which pseudo anonymization could take place. Since this is one of the ways through which Big Data is sourced, it is necessary to regulate the same. An example of Facebook holds good for numerous other websites and applications of companies, tele medicinal apps and so on, where it is promised of not selling personal information, but later sold off under the disguise of anonymization.

4. Need for Strong Encryption and Protection of Obtained Data

Another observation was the unintentional effect of Big Data on consumers. Various companies mine the data in order to facilitate their business. But they lack in securing such data collected. Poor security systems can also lead to data leak, whose loss cannot be priced. Misconfiguration issues are far too common for the healthcare sector, which already is being pummeled by cyberattacks. One wrong click and tens of thousands to millions of patient records can be breached. Med Evolve was the biggest misconfiguration breach in the last two years. While the company recently began notifying 205,000 patients of the error, a

[85] M. Douriez, H. Doraiswamy, J. Freire & C. T. Silva, *Anonymizing NYC taxi data: does it matter.*?, IEEE Xplore (2016), available at https://ieeexplore.ieee.org/document/7796899, last seen on 07/11/2020.
[86] J. Siddle, *I know where you were last summer: London's public bike data is telling everyone where you've been,* Vartree Blogspot (10/04/2014), available at https://vartree.blogspot.com/2014/04/i-know here-you-were-last-summer.html, last seen on 06/11/2020.
[87] Y. De Montjoye, L. Radaelli, V.K. Singh A. & Pentland, *Unique in the shopping mall: on the reidentifiability of credit card metadata*., 347 Science 536, 539 (2015), available at https://dspace.mit.edu/bitstream/handle/1721.1/96321/UniqueInTheShoppingMall_draft.pdf?sequence=1&isAllowed=y, last seen on 08/11/2020.

security researcher made the discovery in 2018.[88] A group of Long Island providers and Middletown Medical in New York also made a similar mistake this year.[89]

When the professional development system at Arkansas University was breached in 2014, 50,000 people were affected.[90] That's a large number, but compare it with 145 million people whose birth dates, home and e-mail addresses, and other information were stolen in a data breach at eBay that same year.[91] From the perspective of a security professional, protecting Big Data sets is also more daunting. This is partly due to the nature of the underlying technologies used to store and process the information.[92]

Thus, companies must update their databases and avoid misconfigurations. When a company can make the best use of such database, it is an obligation on them to protect and invest upon a security system. Most of the time, it is difficult to trace the actual owner of such databases. Thus, consumers are diminished from the opportunity to sue and get justice, when a potential threat to their privacy arises. Thus, the issue of ascertaining the owners of such websites must be taken up by amendments, while registering companies under their respective company incorporation acts. Also, companies and other associated functionaries must include data and security researchers in their organization to constantly have a tab on the collection and protection system of data.

5. Consumer Awareness and Need for Self-Management

Self-management of online privacy seems particularly important as the law only provides limited privacy protection. First, in many countries, the law

---

[88] *More than 200,000 patients' records were exposed on MedEvolve's public FTP server – researcher,* DataBreaches.net (16/05/2018), available at https://www.databreaches.net/more-than-200000-patients-records-were-exposed-on-medevolves-public-ftp-server-researcher/, last seen on 16/12/2020.

[89] Supra 39.

[90] J. Ryoo, *Big Data Security Problems threatens consumer privacy,* Government Technology (24/05/2018), available at https://www.govtech.com/data/Big-Data-Security-Problems-Threaten-Consumers-Privacy.html#:~:text=When%20the%20professional%20development%20system,at%20eBay%20that%20same%20year, last seen on 16/12/2020.

[91] J. Ryoo, *Big data security problems threaten consumers' privacy*, The Conversation (23/03/2016), available at https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798, last seen on 05/11/2020.

[92] Ibid.

is not fully prepared for modern data processing practices. Even if lawmakers and regulators want to protect privacy, they are struggling with the question of how to provide effective legal privacy protection. Moreover, even if up-to-date privacy laws are in place, enforcement is often insufficient. Regulators have limited resources to make companies comply with the law.[93]

"People value their informational privacy", yet *"they surrender it at the drop of a hat"* by readily sharing personal data in the course of simple daily transactions.[94] Most of the time, consumers online accept to the terms and condition without reading it, and provide their personal information without familiarizing with the privacy policy of such companies. This act of theirs is considered as an informed consent. Companies do mention their intention to utilize the personal information for other purposes of business under such a policy. Thus, the consumers literally give their informed consent for their data to be sold or used for other ulterior purposes.

This means that laws mainly focus on consumers' consent, and lawmakers appear to assume that empowered consumers can make rational, educated decisions in their own best interest. The question, however, is whether people are actually empowered and able to make decisions about giving consent and to protect their online privacy after giving consent. When this would not be the case, it would suggest a need for more effective privacy laws, which rely less on empowering consumers, and more on protecting them.[95]

The paradox, he observes, can be resolved by noting that as long as people do not expect that the details of their health, intimacies and finances among others will be used to harm them in interaction with other people, they are content to reveal those details when they derive benefits from the

[93] Sophie C. Boerman, Sanne Kruikemeier, Freidrik J*, Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data,* Sage Journals, 1, 2 (2018), available at https://journals.sagepub.com/doi/full/10.1177/0093650218800915, last seen on 16/12/2020.
[94] R. A. Posner, *Privacy, Surveillance, and Law*, 75 The University of Chicago Law Review, 245, 251 (2008), available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5655&context=uclrev, last seen on 08/11/2020.
[95] Supra 93.

revelation.[96] Thus, consumers should read the policies before consenting to it. Modern consumers, though being well aware about ongoing privacy and data issues must take a step forward in self-regulating their actions.

VII. CONCLUSION

In the present digital and technological era, the roles of the public and private sectors have broadened alongside the increased demands for improved and efficient services from the consumers. The private sector players in order to establish broad customer bases and to achieve profits, collect, store and process the personal information of the consumers to analyze existing and evolving trends. Similarly, the government has inculcated e-services as a part of better and reformed governance. To achieve competent, productive and effective governance, the government needed to take advantage of the technology. Big Data analytics was the solution that both private and public sector players instilled as an integral part of their services.

The benefits of Big Data are being harnessed at every stage and aspect of the service providing process. In the process of gathering different sets of data to coordinate services in a proper, smooth, quick, and effective manner, the most intrinsic right of the citizens i.e., privacy was forgotten. Consent of the citizens and the gravity of its requirement has been overlooked. Lack of specific regulation contributes to the negligence regarding consent.

With new challenges being built on, it has become difficult to cope with evolving technological advances. A specific legislation which is explicit regarding the aspects of consent, the wide scope of definition of consumer, precise regulation on anonymized and pseudonymized data is the need of the hour. The government must also keep the changing technological developments on Big Data and the possible impact the consumers in mind while formulating a specific regulation on Big Data analytics.

[96] Supra 52.