VOLUME – II
DEC 2018

LAW AND TECH TIMES

Special Edition on Data Protection and Privacy

RAJIV GANDHI NATIONAL UNIVERSITY OF LAW, PUNJAB
RGNUL
PATIALA
KNOWLEDGE EMPOWERS

IN THIS EDITION OF THE NEWSLETTER:

THE IMPACT OF BIG DATA ON THE WORLD[1]

Big data is the new game changer in the field of data science, which has revolutionized user behavioural analytics and market research completely. Big data is that new tool in the skill set of data science which has allowed for new avenues to open in the scheme of human asset planning and social research as a whole. But how does big data work? What legal implications doe it bring along with it? This article aims to break down this phenomenon of data science in a systematic manner.

What is Big Data and How Does it Work?

Big data refers to any and all forms of data sets that are too huge to be processed via conventional methods and tools. These data sets are collected in real time from a wide variety of sources and then are processed to detect patterns and information keys among them to allow for new information to be induced from a very vast and otherwise haywire piece of data set. This information is then used by various agencies and organizations to get a deeper insight into the behavioural trends of any aspect of human assets[2].

The patterns that are collected via big data are often collected through sources like social media inputs, public user information, statistical trends in stock markets etc. this data is often available in a very short amount of time and need not be collected in a dedicated manner, with it being available almost simultaneously as people carry on with their day to day interactions and activities, generating such data. Big data has major applications across fields such as marketing research, buyer's trends, social research, policy frameworks etc. Consumer's data is collected from various sources such as online portals, and translated into readable patterns of voting trends that are currently emerging. These trends help the political associations to campaign accordingly to the public trends.

The Impact of Big Data Around the World

With the advent of big data, there have been tremendous improvements across multiple fields which rely on data as a form of input. Big data has created a revolution in the field of **security applications**, with new algorithms being generated based on the breach of previous ones, allowing the security systems to train themselves so as to prepare better for the next breach thus allowing for a more secure interface over many services, be it the internet, or system security in general.

Cloud computing has become more accurate and efficient owing to the ability to process huge amounts of incoming data and generating a pattern based processing technique which allow for it to function in a much more independent and intelligent manner than ever before.

The field of **artificial intelligence**[3] has also reaped credible amount of benefit from big data, with machine learning and genetic algorithms being easier to program and train with huge data sets which allow for neural networks to be trained in real time in a non-supervised manner. Other fields of application include **scientific research**, where big data is used for multipurpose analysis of events, be it cosmology or weather forecasting, **product placements**, where big data plays an important role by allowing for companies to figure out how the

---

[1] Sanidhya Parashar, II[nd] year, Rajiv Gandhi National University of Law, Punjab

[2] Martin Hilbert and Pricilla Lopez, *The World's Technological Capacity to Store, Communicate, and Compute Information*, available at, http://www.uvm.edu/pdodds/files/papers/others/2011/hilbert2011a.pdf

[3] Kristian Kersting, *From Big Data to Big Artificial Intelligence*, available at, *I*https://link.springer.com/article/10.1007/s13218-017-0523-7

average user responds to their product, thus allowing for them to produce according to the user's needs etc.

Various countries deploy big data owing to its plethora of applications. **China**[4] uses big data to collect and monitor its population and gather biometric data. **India** on the other hand utilized the data gathered from electoral response to determine how the public responds to election campaigns. This technique allowed for the BJP to gain an upper hand in the 2014 elections. India like many other countries uses big data in policy framework formation via its think tanks like NITI Ayog which determine the course of action in any given scenario using the insight that big data provides. Various other countries like **Singapore** and **Australia** use big data as a means for analytical revision which allows them to formulate better strategies for the future.

Breaches And Privacy

With these technological advancements in data science, the concern for information privacy was raised due to numerous reports on the extent of data mining that might take place. With the onset of the Facebook Cambridge-analytica scandal[5], it throws some light onto the matter, just how much is this data worth in the wrong hands and what part of an individual's data is actually left to his privacy, with corporations willing to sacrifice personal liberty and privacy of users to further their own gains. Various countries have different provisions so as to protect the data of their citizens and not to allow for their privacy to be breached.

India, with the recent judgment in the case of **KS Puttaswamy v. Union of India**[6], had concluded that an individual has his right to privacy protected as a fundamental right. This paved the way to strengthen the scheme of data protection in the Indian ecosystem**. Singapore**[7] on the other hand comes in with its own Personal Data Protection Act (PDPA) which governs the analytics and data mining that takes place and the manner it takes place in. **Britain** has their Data Protection Act[8] (DPA), which governs how an individual's personal information is used and processed.

Towards The Future

Big data remains a promising technology on planning for the future. It has helped improve the existing fields of research and continues to transcend boundaries and breaking grounds across platforms. With the advent of new data protection schemes, the one existing shortcoming of big data on data privacy can soon be overcome and it will allow for a more ethical and fruitful utilization of this revolutionizing technology.

[4] *China: Big Data Fuels Crackdown in Minority Region,* Available at, https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

[5] Court Stroud, *Cambridge Analytica: The Turning Point In The Crisis About Big Data,* available at, https://www.forbes.com/sites/courtstroud/2018/04/30/cambridge-analytica-the-turning-point-in-the-crisis-about-big-data/#2f53016748ec

[6] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. WRIT PETITION (CIVIL) NO 494 OF 2012

[7] Ruth Ng, Singapore Smart Nation – *How the law is changing with big plans for Big Data,* available at, https://www.taylorvinters.com/article/singapore-smart-nation-how-the-law-is-changing-with-big-plans-for-big-data/

[8] Data protection act, 2018, available at, https://www.gov.uk/data-protection

DO YOU KNOW: OTT MEDIA SERVICES?

The term 'OTT' or Over-the-top media services refers to digital content providers who deliver multimedia material to users over the network services of Internet Service Providers (ISP).the network providers are not in control over the copyrights or distribution rights of the media provided by the OTT players. this is contrary to the purchasing and renting model of media content directly from the Internet Service Providers. In simple words, OTT content refers to the third-party content that is distributed to end-users through ISPs.

We have been using OTT content, knowingly or unknowingly, over the years through our PCs, smart phones and tablets. the creation of OTT players has led to conflict with traditional players who offer overlapping services. For example, think about an OTT player like Netflix coming in conflict with your cable service provider. Other OTT players include Apple TV, Amazon Prime, Skype, etc. although OTT customers make up a small percentage in today's world, their number is going to skyrocket in the coming years with the increase in internet coverage and access to e-devices.

GDPR AND OTT SERVICE PROVIDERS

The General Data Protection Regulation (GDPR) came in to force in the European Union on May 25, 2018. The new regulations have majorly impacted digital industries including OTT service providers. In the recent past, most digital industries including OTT players have become data-driven. Hence, the GDPR will have a significant effect on the functioning of OTT service providers.

Failure in compliance will attract hefty penalties. According to the Wired, "If an organization doesn't process an individual's data in the correct way, it can be fined. If it requires and doesn't have a data protection officer, it can be fined. If there's a security breach, it can be fined. "[9]

Online indicators like IP Addresses and cookies are considered as personal data under the GDPR. These indicators are used by OTT players to provide personalized content recommendations, targeted advertising and for the distribution of streaming content itself. The GDPR has very strict guidelines regarding the collection, relevancy and legal justification for OTT players in control over users' personal data. So, OTT service providers have to be much more careful while collecting and processing personal data and will be held to a greater degree of accountability.

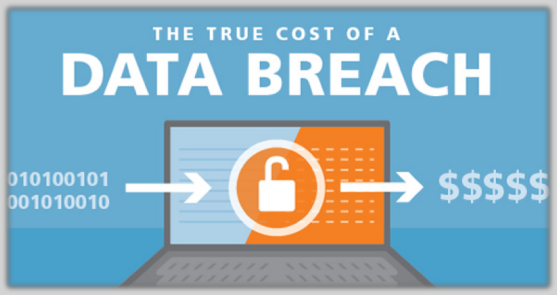
Consumers will have greater control over their personal data, more than they ever had. User consent is a key area of focus in the GDPR. OTT players will also have to guarantee additional rights to the users, including the right to be forgotten and the right to data portability. Customers will also have more rights to access their data and see what is being kept on them. Requests can be made to the OTT service providers for access to data, against which a nominal fee may be charged by the businesses.

With the coming to force of GDPR, applications using Artificial Intelligence will be under much more scrutiny. AI is used by OTT players to provide personalized recommendations to users and to provide targeted advertisements by using algorithms which gauge user preferences. GDPR seeks to bring greater transparency to data collection and processing and as a result, OTT businesses will have to inform their users about the process of data.

[9] https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

EXTREME DATA BREACH INCIDENTS IN INDIA

A survey had been conducted by defence grade technology maker Thales, where it revealed that at least 75% of Indians faced data breach than compared to 67% globally. Cook, the South-Asia director, said that the same is occurring because India has been spending the budget either at the wrong places or focused only at the end points.[10] Another study had been conducted by IBM and the Ponemon Institute, where it revealed that data breach cost in 2017 had shot up to ₹9.73 crore from ₹8.85 crore, making India the most targeted country for data breaches in the world.[11]



As revealed by global player in digital security, Gemalto, in 2017 the Breach Index Level recorded 203.7 million data records to have been compromised in India.[12] "Breach level index is a global database that tracks data breaches and measures their severity based on multiple dimensions, including the number of records compromised, the type of data, the source of the breach, how the data was used, and whether or not the data was encrypted."[13] In fact, Data Threat Report, 2018, also highlights the gravity of the situation by emphasizing the need for change in security strategies to prevent increase in data breaches.

An increase can be seen in the organisations meticulously planning to increase their budget in IT security, however, the survey noted that it is the Aadhar alone which is able to drive the organisations towards the same than any other geographical or vertical market sector. Though, as of now, Indian companies are employing the advances and latest technologies to tighten IT security, however, they are still in the struggling phase to cope up with identifying and containing data breaches, leaving upon loopholes to curb the same.

GOOGLE UNLEASHES IMAGE DETECTION AI

Google has recently announced that is to employ a new AI technology that will help in detection of Child Sexual Abuse Material (CSAM) online. It acknowledged that the spread of such content online is one of the worst abuses imaginable.

This technology has been brought in with the aim to combat online spreading of content of child sexual abuse. This new tool is based on deep neural network which will be made available for free, to NGOs and other industry partners via a new Central Safety API service that could be offered upon on request.[14] AI technology employed, is hoped, to significantly help the service providers, NGOs and other industry partners (including tech firms), to improve CSAM efficiency and reduce viewer's exposure to such content.

[10] Data Breach Incidents in India Higher Than Global Average, The Indian Express, available at https://indianexpress.com/article/technology/tech-news-technology/data-breach-incidents-in-india-higher-than-global-average-5272118/.

[11] Varun Agarwal, India- The Most Targeted Country for Data Breaches, The Hindu, available at https://www.thehindubusinessline.com/info-tech/india-the-most-targeted-country-for-data-breaches/article8907519.ece.

[12] Gemalto, 203 million records breached in India: Report, CSO Online, available at http://www.csoonline.in/media-releases/203-million-records-breached-india-report.

[13] Ibid.

[14] Google's New Tactic to Fight Child Sexual Abuse: AI, The Economic Times, available at https://economictimes.indiatimes.com/magazines/panache/googles-new-tactic-to-fight-child-sexual-abuse-ai/articleshow/65669835.cms.

This technological advancement will be able to quickly identify new images, which means it will be able to identify children who are abused and protect them from further abuse. Many tech companies are also of the opinion to let AI detect contents of nudity and abusive comments as well.

In the trial, the tool was a success since it helps viewer find and act on 700 percent more CSAM content over the same time period.[15] This google project stems from its cooperation with some of the partners like Internet Watch Foundation (British-based charity), the WePROTECT Global Alliance, Technology Coalition, etc. in fighting online the child sexual abuse.

IMPACTS OF GDPR ON AI

Artificial Intelligence (AI) sector is a promising one and altogether a new generation of technological advancement which is highly disruptive and productive for the Industry 4.0. AI is a constellation of technologies performing different cognitive functions. AI is a progressively improving technology which feats on data for understanding the patterns better. Having been existed for some time now it has become a reason of rapidly increasing computational power in industry (Moore's law phenomenon) leading to the point where AI market will surpass $100 billion by 2025. AI is significant as it will transform the medium of interaction between humans and technology resulting in overall societal advantages such as inventiveness, innovation and confidence.

With all the advancement in AI industry, it brings a lot of concern for regulators across the different jurisdictions. One of the major concerns is use of data in AI. This is making the regulators hesitant in order to allow AI start-ups to initiate any kind of large-scale activities based on AI technology. AI start-ups are soon going to hit a major impediment as the European Union's GDPR is in effect now. The GDPR had been enforced by European Union (EU) to form a strengthened, integrated and unified data-privacy mechanism. It aims primarily to provide the EU citizens an instrument of more control over their personal data and its protection. It provides a framework in which individuals will have liberty to ask questions that how the companies or institutions are processing and storing their personal data. The challenge of full accountability to consumer as strictly put mentioned by the GDPR makes the collection of data by more difficult impacting the AI start-ups which are absolutely dependant on varieties of personal data for machine-learning initiatives.

The concerns of AI-start-ups can be explained as two-fold. Firstly, processing of data has direct legal effects on the customer, such as credit applications, e-recruitment or workplace monitoring. The GDPR will completely limit the usefulness of AI or these purposes as the Article 22 and Recital 71 strictly provides for the requirement of explicit consent for each and every unit of data that is used making the functioning of the market slower. Secondly, the algorithms that the AI developers use for the application, evolve in a way, making it complex and not easily understandable, thereby, difficult to regulate. The way out for AI start-ups seems to be in the organisational procedures that can standardise the obtainment of consent for the governance of the data within a well-structured data management framework. The GDPR compliance would require a fixed policy of filing an automated appeal to

[15] *Ibid*.

consumers from the AI developers while processing the huge amount of data.

Illustrating this, it is required that if a consumer is denied the service by any AI application, developers should provide a chance to know the reason to that consumer i.e. an appeal. It is worth to mention it is humans that have created, modified and implemented AI technology and they also have the potential to make it compliant and moderate according to the reasonable considerations of regulators. GDPR is not an evil for AI applications but it is just a regulatory initiative with which if AI technology develops, it will get more confidence of the potential consumers.

LEGAL DEVELOPMENTS

CAREFIRST V. ATTIAS (U.S. SUPREME COURT)

In a recent development regarding the data breach, the U.S. Court of Appeals in the D.C. Circuit has come out with a judgement dealing with the issue of the leakage of data of 1.1 million policyholders.[16] The case dates back to 2014, when the Health Insurer Company Carefirst Inc. suffered a data breach that compromised the personal information of approximately 1.1 million policyholders.[17] Affected Customers brought a lawsuit against Carefree alleging that it had violated a number of laws by failing to safeguard their personal information leading to a increased risk in the field of data theft in the United States.[18]

The legal battle started in 2014 when petition was filed against Carefirst on the grounds of negligence in the handling of the data of the 1.1 million customers.[19]

CareFirst moved to dismiss the complaint on the grounds that the plaintiffs lacked standing, because they had not alleged any instances of identity theft. On one hand, when the counsel for Carefirst was arguing here, on the other hand, a gross violation of the personal data was alleged by the people concerned.

The Court was moved by the arguments of the Health Insurer Company as they were successful in convincing the Court that the plaintiffs' had failed to allege an "injury in fact" that is concrete, particularized and imminent as was iterated in the Supreme Court Precedent of *Spokeo v Robbins*.[20] The plaintiffs had appealed to the United States Court of Appeal for the District of Columbia Circuit which reversed and remanded for the future course of proceedings holding that the plaintiffs had plausibly alleged a risk of future injury because it was at least plausible that the cybercriminals had the intention and ability to use the stolen data for the sinful purposes. The defendant CareFirst initially succeeded in obtaining dismissal of the data breach claims on standing grounds.[21] CareFirst argued that plaintiffs had alleged no injury beyond the statutory

[16] Carefirst Data Breach Suit Properly Tossed, D.C. Circuit, Jeff Sistrunk, Q law 360.
[17] Maryland Court dismisses Carefirst Data Breach Lawsuit, Elizabeth Snell, Health IT Security.
[18] Reforming the U.S. Approach to Data Protection and Privacy, Nuala O' Conor, Council on Foreign Relations.
[19] Data Belonging to 1.1 Million Carefirst Customers Stolen in Cyber Attack, Kate Vinton, Forbes.
[20] Spokeo Inc. v Robbins, How the Supreme Court Court could transfer Consumer Class Actions, Westlaw Journal Class Action.
[21] The Dark Web—the Next Frontier in Data Breach Standing Analysis Amid a Deepening Circuit Split, Andrew B. Serwin, Purvi G. Patel, Alexandra Laks, CyberSecurity and Privacy.

violations purportedly arising from the breach.[22] In fact, three years later, none of the plaintiffs had suffered any concrete harm resulting from the breach. The trial court agreed with CareFirst's argument that without a concrete injury and without an imminent risk of substantial harm, plaintiffs did not have standing to sue simply because the breach had exposed their personal data.[23] Moving back to the initial stages of the case, The District Court had ordered in the favour of Carefirst which afterwards was reversed by the U.S. Court of Appeals for the D.C. Circuit, which held that plaintiffs had held a risk of future injury because it was at least plausible that the cyber criminals had the intent and ability to use the stolen data for wrongful purposes.[24] It was henceforth that Carefirst filed a writ of Certiorari in the Supreme Court of the Land, which has at last denied the petition leaving the ruling of the U.S. Court of Appeal for D.C. Circuit in favour of the Plaintiffs.[25]

Hence, it is now in the hands of the Apex Court of the land to determine whether the consumers are at an imminent risk if their data is exposed, or is there some parameter to be set by the Hon'ble Court that determines the leakage of data. The Supreme Court needs to take into consideration many issues at a certain time, looking upon the evidence at the same instance of time. The Apex Court now has an urgency to adjudicate upon the claims of theft of the data and its breach.

THE PERSONAL DATA PROTECTION BILL, 2018

Amidst the debate between the Sri-Krishna Committee reports regarding the Data Protection and its recommendations, in an important improvement under the Personal data Protection Bill, 2018 the Union Legislature is planning to make a two-fold change.[26] At the first place, where the Bill introduces the concept of *Extra-Territorial jurisdiction*, i.e. along with the lines of the GDPR, secondly it also imposes penalties.[27]

Under Section 68 of the Bill, The Adjudicatory officers are required to award penalties for the violation of the data protection law, wherein two levels are setup.[28] On one side, the penalty amounts to Rs.5 crores or 2 percent of the total worldwide turnover, the second is up to 15 crores or 4 percent of the world-wide turnover.[29]

The Adjudicating Wing is responsible for all the penalties as per the concerned section of the Act. In addition to this, the Bill also lays down provisions for the criminal intent, i.e. on reckless violation of the law with criminal intent. The Bill makes it clear that anyone found with such offence with criminal

[22] Attias v Carefirst, United States Court of Appeal, Districts of Columbia Circuit.
[23] *Ibid*.
[24] Supreme Court denies Cart Petition in Carefirst v Attias, Philip N, Yannella and Edward J. McAndrew.
[25] Attias v. CareFirst: CareFirst Petitions for Cert to Decide Standard of Harm in Data Breach Cases, Amy Aixi Zhang, Harvard Law School.
[26] Justice Sri-Krishna committee submits report on data protection, Surbhi Agarwal, The Economic Times.
[27] Srikrishna committee exceeds its brief on data protection, Rajrishi Singhal, Livemint.
[28] Our Comments on the Expert Committee's White Paper on Data Protection Framework for India, Data Protection Framework.
[29] *Ibid*.

intent shall be imprisoned up-to 5 years or a fine of 3 lakhs.[30]

Other penalties in the Bill include failure to adhere to data protection principles, processing without a lawful basis of processing, data localisation and cross-border transfer requirements, penalty in relation to security safeguards and data breach notifications. All these penalties under the Bill are in addition to those provided under the IT Act and other such Acts.

DA VINCI SURGICAL SYSTEM

Artificial Intelligence is the simulation of human intelligence by machines involving the superlative memory, decision making power, exponential speed of action and a lot more. But being a human is not confined to intelligence only but to get socialize with human beings and to live within its own limits. Machines do not possess the inner conscience and ethics which could help them to distinguish between what is right or wrong.

Intuitive Surgical Inc. is an American company that is committed towards developing the robot assisted technologies, tools and services which can be used in surgeries. The core innovation of the company is the "da Vinci Surgical System" often described as "robot surgeon" was introduced in the year 2000 that promised to reduce pain and complications and to lessen the recovery times.

It can be used for gynecology, urology, thoracic surgery, etc. The 3 dimensional view of the area and more précised handling of the instruments. The system was capable of reaching the places which was not possible for human hands. The robot was not developed to replace the laparoscopic surgery but to expand its application. The system has three integrated sub-systems. The surgeon is always in control of the system. But since it is a machine, sometimes due to the malfunctioning of the system, there is need of larger incisions in order to complete the surgery manually. The system is in news from the past couple of years. The report published by the National Institutes of Health in 2016 stated that over 1.75 million robotic procedures have been used across the US and da Vinci Surgical System is the only one which has been approved by the Food and Drug Administration, America.

FDA in the year 2013 sent the warning letter to the Company to remedy the certain violations of its regulations. According to its investigation it found that the various components of the system were misbranded. Around 70 people were claimed to be killed due to the malfunctioning of the system as reported by Bloomberg, also according to the NBC news, FDA conducted an inspection and found some microscopic cracks in the system which have led to "sparking" that damaged the tissues and the organs surrounding the surgical area. A portion of the system's arm extends off-camera beyond the surgeons view and it is this area where the problem is occurring. Around 50 lawsuits have been filed against Intuitive alleging fatal injuries and wrongful deaths occurred due to the da Vinci complications. Despite the injuries caused by the system and its high price, the use of the robotic technology is still on rise with an increase by 16 percent in the second quarter of 2016 contributing $700 million for the 2016 fiscal year.

TRAI RELEASES RECOMMENDATIONS ON DATA PRIVACY

The Telecom Regulatory Authority of India (TRAI) released its recommendations titled 'Privacy,

[30] Our Privacy's Worth, Shankar Narayanan, The Hindu.

Security and Ownership of Data in the Telecom Sector' which are applicable on telecom and internet service providers.

The recommendation has detailed the importance of data protection guidelines in the telecom sector and also given an analysis on the efficacy of the existing framework.

TRAI has included Telecom Service Providers (TSPs), OTT players, operating systems and apps in the digital ecosystem which it envisages to be regulated by its recent recommendations. Although it remains to be seen whether all the other services will come under the purview of TRAI considering TRAI is empowered by the Telecom Regulatory Authority of India Act, 1997 to include entities operating in the telecommunication environment only. The core issues discussed in the recommendations include personal data and data ownership, sufficiency of existing data privacy framework, user consent, data security. In addition to these core issues TRAI has also discussed the possible use of the Blockchain Technology by TSPs. The TRAI recommendations state that ownership of personal data lie with the users from whom the data has been collected. The Recommendations considers digital businesses collecting and processing user data to be 'mere custodians', and hence, have no primary rights over the same. This is one of the various aspects in which the TRAI recommendations track the General Data Protection Regulations recently implemented in the EU.

RBI REGULATIONS IN CONTRADICTION WITH GDPR

Recently, a fintech start-up 'PhonePe', Flipkart owned, released a statement that wherein it stated that one can unlink the bank account and log out of the app, however, not be able to delete the account from the app. The only resort is the option to block the account. Fintech is an upcoming industry that uses technology in improving activities in finance. This further ignited the spark that had already been doing rounds regarding Fintech companies not be able to delete customer data under current laws. RBI and Income Tax regulations have mandated all financial institutions to maintain customers' records for a period of 10 years. For suspicious transactions, the period goes up to 15 years. These regulations come in clash with GDPR, as enforced by European Union from 25 May, 2018.

The regulations have not only made stricter rules in regard to use of data of people without their consent, but its enforcement has made people aware across the globe of their personal security information.

Therefore, fintech companies have come in fix while complying with domestic laws but then be in contravention to GDPR guidelines. It will be an interesting to study the path these fintech companies will be discovering and using in order to find a safe route between the points of clashes and survive in the world of stricter regulations.

DO YOU KNOW: A STEP TOWARDS SUSTAINABLE FISHING?

The 'SMARTFISH-H2020' project, co-ordinated by SINTEF Ocean in Norway, draws on research from universities in Norway, Denmark, Turkey, France and Spain, along with Institutes and Industry partners across Europe. Along with them are included the Centre for Environment, Fisheries and Aquaculture Science (CEFAS), Safetynet Technologies Limited, etc. The project aims to develop and test before rolling out a suite of high-tech systems that would be optimising efficiency to reduce ecological impact of fishing. This technology would also be enabled to collect data and provide evidence regarding fishing regulation compliance. It seeks to develop image technology such as on-board CCTV and smartphone applications to automatically quantify the fish catch. "It will help those in the fishing industry make informed decisions and lead to better economic efficiency, as well as reduce unintended fish mortality. It will also help provide new data about fish stocks and automatically collect catch data to ensure compliance with fisheries management regulations."

The makers of this technology also emphasize on its utility for not only the fishermen, but also for research and policy making. The developments in this sphere will enable the analysts to contemplate upon the decisions for pre-catch, catch, and post-catch phases of the fishing process. Apart from this upcoming technology with the use of AI, England too has devised a technology to regulate the marine environment during groundfish season. This cost-effective measure of electronic monitoring ensures that the fishermen are not catching more fish than allowed.

FACEBOOK AND GOOGLE HIT WITH BILLION DOLLAR LAWSUITS

The General Data Protection Regulations came into effect on 25th May, 2018 across Europe and on the day of implementation, Facebook and Google were hit with lawsuits accusing the companies of coercing users in to sharing personal data. These lawsuits filed by a privacy activist from Austria seek to fine both companies $8.8 Billion.

The new regulations make it mandatory for businesses to provide users with complete information and seek clear consent for personal data collection. Facebook and Google have come up with new policies to be GDPR compliant but the activist who filed the lawsuit feels that the policies are not good enough and force the users into an all-or-nothing agreement which is violative of GDPR guidelines on user consent regarding data collection. Michael Schrems, the man behind the lawsuits told *The Financial Times*, that the existing policy is not GDPR compliant. "They totally know that it's going to be a violation," he said. "They don't even try to hide it."[31]

Schrems says the new rules are tough enough to prevent the kind of data scraping that Cambridge Analytica before the 2016 U.S. election. He's taking legal action to ensure GDPR is properly enforced.[32]

"If we enforce the properly, we can actually get a balance in this digitalized age," says Schrems. "In the end, you should be able to use Facebook without worrying 24/7 about your data," he added.[33]

THE CALIFORNIA CONSUMER PRIVACY ACT, 2018

In a series of efforts of law-making for the purposes of the protection of consumer's personal information or privacy, the people of California are set to undergo a

[31] https://www.ft.com/content/01d2d094-5f96-11e8-9334-2218e7146b04.

[32] https://money.cnn.com/2018/05/25/technology/gdpr-compliance-facebook-google/index.html.

[33] *Ibid*.

ballot initiative in the month of November.[34] The California Consumer Privacy Act shall be implemented to give the residents of California a right to enquire from the Businesses about the categories of personal information with respect to third parties.[35]

The Act marks a clear distinction on the personal information that can be enquired about within the ambit of this Act. Personal information includes the name, address, social security number, government issued identity number, biometric data and geolocation data.[36]

The Act engrosses within it the right to know, wherein the personal information the business has collected about the consumer and the categories of personal information sold or disclosed to third parties has been included.

The application of the Act is also valid contrary, i.e. the disclosure of personal information of consumers to concerned third parties. Among many methods to enquire about the business, the disclosures must be made within 45 days of the receipt of the request using one of the methods specified in the Act.[37] Moreover, with regards to the exception, the covered businesses will not be required to make the disclosures in case of the contract with another person barres the portrayal of personal information other than performance specific information.[38] The Act specifically carves out an exception for minors too, where upon satisfying 2 of the prescribed conditions, the minor shall be able to authorise the sale.

The main catch of the Act is that it has layered on sections in the favour of customers, wherein upon a verifiable request by the customer, the personal information of the customer shall easily be deleted. The Act is to come into effect into early 2020, and we expect an optimistic change in securing the privacy of the people of California.

US WEBSITES BLOCKED IN EU POST GDPR

The General Data Protection Regulation (GDPR) came in to force in the European Union on May 25, 2018. The new regulations have significantly impacted implemented businesses in the digital ecosystem including major US media companies. Dozens of US news websites have been blocked as a result of non-compliance with the GDPR which include biggies like *The New York Times, CNN, The Los Angeles Times* and *The Chicago Tribune* among others.

Most organisations had two years prior to the GDPR's implementation to fall in line but they have rejected to comply with the privacy policy as required by the new regulations. The GDPR was rolled out to grant users more control over the data they share and it's not just tech companies which have to comply with the same. Media companies which provide their journalism services on the internet also collect user data and are hence required by law to comply with the regulations.

[34] Analysis, The California Privacy Act, 2018, Lothar Determann, Privacy Tracker.
[35] Californians for Consumer Privacy Applauds Successful Passage of Groundbreaking Legislation, Robin Swanson, General Consultant and Campaign Manager for the California Consumer Privacy Act.
[36] Personally Identifiable Information, The Grossary of Education Reform.
[37] California Consumer Privacy Act Signed, Introduces Key Privacy Requirements for Businesses, Hunton Andrews Kurth LLP, Privacy and Information Security Law Blog.
38 Ibid.

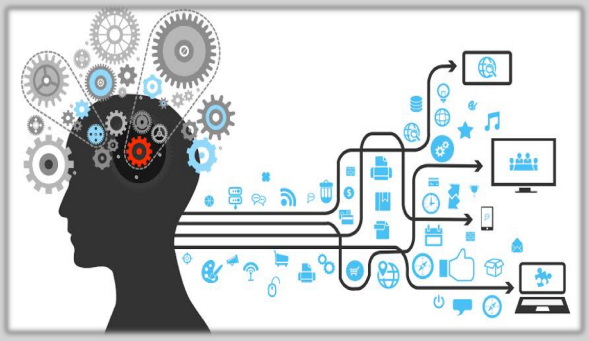
All organizations which collect and process data of EU citizens, including banks, transport networks, e-retailers, etc have to comply with the new regulations. May 25th 2018 was the last day for all businesses comply with GDPR, but surveys showed that anywhere from 60 to 85 percent of companies said that they're not ready to be compliant.[39]

The European Union regulators are showing no signs of leniency. The reaction to the blocking of news websites have been mixed, with some arguing that the GDPR is too burdensome while others say that the media companies had 2 years to get their act together and should have complied as is mandated by the law.

MANTHANA: AN INDIGENOUS INNOVATION

Artificial Intelligence (AI) is slowly changing the healthcare world. A technology giant Google has partnered with the Dutch University to use the branch of Artificial Intelligence (AI) to treat breast cancers and to provide better healthcare facilities to patients. An Indian based startup SigTuple is doing the same thing in bringing accountability and accuracy to the healthcare world.

The startup has been selected among the top 10 finalists who will participate in the Google's Demo Day Asia, scheduled to be held in Shanghai in the month of September. The startup creates Artificial Intelligence based solutions automating the health care screening has come up with an Artificial Intelligence (AI) based platform: Manthana, which analyses the visual medical data. The innovation has eliminated the need of experts to physically present during the patient's examination.



It has helped the company to work on the analysis of peripheral blood smears, urine, semen, chest X-rays and retinal scans. It has helped the healthcare world in finding abnormalities which will be further investigate so as to detect diseases.

It includes features such as: ingestion of visual data such as videos and images, classifying various objects, memory to store data which can be used to predict disease conditions in future, providing reports backed by visual evidences and to generate feedback for the same.

The company is currently working to scale Manthana so that it can churn large amount of information and bring intelligence out of it. The motive of the company is to provide quality healthcare facilities to the common man.

[39]https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542.

DO YOU KNOW: MINNIE, A READING COMPANION.

Researchers at the University of Wisconsin- Madison have developed a robot named *"Minnie"* which can be a reading companion for the middle school kids. It is a foot tall machine with a humanoid face, and its blue eyes blink to convey emotions like thoughtfulness. There is a camera installed which enables it to see pages. There is also a microphone attached which enables it to hear a book being read. The robot can make the task of reading more exciting and interesting by making it a group activity.

It can help parents who are so busy with their own work that they cannot engage with their children to help them to read effectively. The researchers claimed that the robot has the ability to react, cajole, summarize things and can appear thoughtful which does not mean that the robot has emotions of its own; it is just a pre-programmed responses. The researcher said that the robot is not a social companion to which you can have a peer-to-peer conversation. But it is programmed to be a good listener which can help the children to inculcate interest in a particular subject.

Researchers said that they have designed a two week reading programme in it which includes 25 books involving a range of reading skills and story complexities. The students get more attracted towards the robot while reading with it during the course of two weeks.

NEW ZEALAND'S NEW PRIVACY LAW

In the light of the increase in the breach of the online personal data of the individuals, the Legislature of the Nation has started to get attention of EU's GDPR.[40] Recent data has proved that New Zealand has to lift its game on Data Protection. In New Zealand, currently there is no law requiring companies like Z Energy, Linked In or vector to tell New Zealanders if their data has been leaked.[41]

Legal Analysists of New Zealand are trying their best to lift their privacy laws as the risk factor involving is too high at the present stage in the country.[42] The citizens' data is at risk in New Zealand, and a major factor involving it is the trade done by the Companies of New Zealand. If New Zealand does not make a law soon, then each of the Companies would have to have their own compliance.[43]

As New Zealand has their major businesses between Australia, Canada and European Union.

The Justice Select Committee has now met to define a new definition of Privacy for the protection of personal data for individuals. The Act was first passed in 1993, and now at this stage of time when people are sharing things amongst themselves, it is difficult to determine for the authorities the authenticity of the data shared by the people on the internet.

The bill also makes sure that public consumption of the day-to-day news is not restricted to some forms of media. Thus, under the current act, media are exempt from certain provisions for the purposes of gathering and reporting news and current affairs, but only the traditional media and ways of imparting that news. The Bill is expected to continue for the freedom of the media.

[40] New Zealand: Internet NZ calls for NZ to lift its game on privacy, Press Release.
[41] The New Rules on Consumer Data and Privacy, NZ Business.
[42] New Zealand urgently needs to get the Privacy Bill right for everyone's sake, says Internet NZ, Sara Barker, Security Brief.
[43] GDPR Compliance in 4 steps, Bianca Mueller.

AADHAR: A BREACH OF PRIVACY

It won't be surprising to say that the Apex Court of India has done a phenomenal job in delivering judgements that might not only shape the modern India but also help resolving the major issues that deal with the question of individualism. It's been a matter of discussion if government can access our private information in the namesake of governance. The need of the quantum of interference of the government in the private affairs and information was not defined. The question of privacy being a fundamental right was left unanswered until K.S. Puttaswamy & Anr. v. Union of India. The case was monumental one since it helped making Right to Privacy a fundamental right.

Recently, the fate of Aadhar saw a big turnover when four prominent sections that allowed the government to access an individual's Aadhar details without their permission. Though the majority upheld its constitutionality, Justice D.Y. Chandrachud called Aadhar unconstitutional. In his dissenting judgement he wrote that when biometric data is combined with demographical data like age, address, etc. the probability of it being misused becomes prominent when done in the masses. He said that the issue wasn't the recognition of identity details but the access of third party to these details in order to generate a secondary use of the information. [45]The Sections of the Act that were struck down or modified are-

1. Section 33(2) [disclosure of Aadhaar Information to an officer not below the rank of Joint secretary to the Government of India]- Struck Down
2. Section 33(1) [disclosure of information on the basis of a court order]- Read Down. It has been held that an individual should be given the opportunity of hearing.
3. Section 57 [use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or anybody corporate or person]- Struck Down
4. Section 47 [no court shall take cognizance of an offense under the Act except on complaint made by UIDAI] – Modified. Should include a provision for an individual to file a complaint.

Tech Involved In Aadhar

The model of Aadhar is based on the concept of Social Security number in USA. Aadhar uses a unique 12 digits identification number that is enough to derive all the personal information that the government requires. Owing to the bureaucratic discrepancies and various kinds of interferences, there could never be a unique proof that would determine the citizenship of a citizen. The call for the same was raised after the Indo-Pak Kargil war with speculations arising that there might be spies, combatants living in India in order to create sleeper cells. Aadhar was an idea to solve all these problems in one go.

The idea of a scheme like Aadhar was to unite an individual to the government through the thread of a digital profiling. This thread was supposed to help the citizens avail all the benefits that the government brought for the ordinary people. The concept was to substitute one document instead of the plenty that we

[45] Mera Emmanuel, *Brazen disregard of our orders: Highlights from dissenting opinion of DY Chandrachud J. in Aadhar*, BAR AND BENCH (Oct. 1, 2018, 1:47 AM), https://barandbench.com/dy-chandrachud-dissenting-aadhaar/.

have, for the ease of the citizens as well as the government.

For the registry of all the Indian Nationals, National Population Registration came into existence. In 2013, during the tenure of the UPA government, *The Economic Times* reported that the UIDIA approached a US based firm called MongoDB for an unspecified database management. The firm is partly funded by the capital firm of Central Investigation Agency (CIA) called In-Q-Tel. If true, the idea is beyond threatening the individualism that any government needs to protect.[45]

Aadhar is a model of USA's Social Security Number (SSN), that helps profiling an individual to determine the income and ascertain the Social Security Credit that they are entitled to based on their financial health. The major difference between the two is that for SSN, the authority does not collect any biometric data. Also, the Aadhar's primary purpose is to authenticate the identity of an Indian citizen. Another major difference that we can witness is in their usage. In USA, both the federal and state government laws strive to protect the SSN of an individual by keeping it extremely private. This is an identity that is supposed to be secretive and be used only when required to hail government welfare benefits. On the contrary, Aadhar number is accessed by all the third parties in the name of extreme protection of individual profiles by 'linking' it to their specific handles. The government made linking of Aadhar to bank accounts compulsory to access them. Almost everything was linked to Aadhar in the past year, SIM cards, money transfer accounts, etc. USA is averse to the idea of linking the SSN to any other welfare scheme be it governmental or private.

Incidents Of Data Breach

In past few years, after the inception of the scheme in masses, people have witnessed various incidents of data breach by individuals to point out at the loopholes that the database carries. The first prominent one was by Baptiste Robert, who hacked the Telangana Service Portal. A mere SQL injection made the website respond with the entire data of individuals that it carried. This data of all the loans, benefits, deposits are tied to the Aadhar card number. In another major incident an Android developer, Abhinav Srivastava fiddled with the Aadhar linked E-Hospital App. He tried pointing out the loopholes but got arrested by the UIDAI. The denial of the authority in the name sake of security policy is beyond devastating.[46] In a huge blow to the government, a *The Tribune* journalist was arrested only because he proved that a mere 500 INR and ten minutes can give you access of any Aadhar profile.[47] Not only this, UIDAI itself accepted the fact there were around 210 websites that made the Aadhar data public. They were Central and State government websites.[48] The multi-layered robust security system has failed miserably in providing adequate protection to the private details of an individual.

Conclusion

We cannot deny the fact that the scheme is one of its kind. The idea of identification of citizens is extremely required in a country like India where crossing the

[45] Lison Joseph, *MongoDB startup hired by Aadhaar got funds from CIA VC arm*, THE ECONOMIC TIMES (Dec 03, 2013, 08.57 AM), https://economictimes.indiatimes.com/news/politics-and-nation/mongodb-startup-hired-by-aadhaar-got-funds-from-cia-vc-arm/articleshow/26755706.cms.

[46] Siddarthya Roy, *Aadhaar: India's Flawed Biometric Database*, THE DIPLOMAT (March 6, 2018), https://thediplomat.com/2018/03/aadhaar-indias-flawed-biometric-database/.

[47] Rachna Khaira, *Rs 500, 10 minutes, and you have access to billion Aadhaar details*, THE TRIBUNE (Jan. 4, 2018, 2:07 AM), https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

[48] 210 govt. websites made Aadhaar details public: UIDAI, THE HINDU (Nov. 19, 2017, 12:38 AM), https://www.thehindu.com/news/national/210-govt-websites-made-aadhaar-details-public-uidai/article20555266.ece#.

border is not big a deal. There is a need of a system like this. But fiddling with what ought to be private is not only unacceptable but also unconstitutional now. If we go by the judgement of Justice Chandrachud and scrap the scheme from the country, it will add up to more chaos and confusion. This is a scheme that is so widely spread that uprooting it is not possible. All we can strive for is segregating the flaws from the very scheme to ensure that a third party is not using the data for meeting its own ends.

[i] Photo: Financial Times. All rights reserved.
[ii] Photo: Brendan Marr & Co. All rights reserved.
[iii] Photo: Robert Halsey, Compliance Gide. All rights reserved.
[iv] Photo: Jamie Condliffe, Gizmodo. All rights reserved.
[v] Photo; African Academic Network on Internet Policy. All rights reserved.
[vi] Photo: Divya Nayak, DazeInfo. All rights reserved.
[vii] Photo: Danish-Thai Chamber of Commerce. All rights reserved.
[viii] Photo: Jeff Powers, IVN. All rights reserved.
[ix] Photo: Mark Wycislik-Wilson, Betanews. All rights reserved.
[x] Photo: Weblizar. All rights reserved.
[xi] Photo: Insight IAS. All rights reserved.

CONTACT:

E-MAIL: lawtech@rgnul.ac.in

Mohak Salva +91 8989870402 Hemendra Singh +91 9872466471