Page 497 - 508

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 2 | Issue 1

2020

Facial Recognition Technology and its Implications on Privacy: An Indian Perspective

RISHABH SEN GUPTA[1] AND UTKARSH AHUJA[2]

ABSTRACT

The world we live in today is seeing the advancement of technology at a rapid pace. What only existed in fiction a few decades back has become the reality we live in today. One such fictional circumstance which might turn into a dastardly reality in the not so distant future is the fear of being under constant vigilance as seen through the portrayal of 'Big Brother' in George Orwell's dystopian fantasy, 1984.

Although the idea might seem farfetched the consequences of facial recognition technology and the threat it may pose in the future should not be treaded upon lightly. If it goes unregulated it may prove to be a threat to the very notion of democracy we cherish thus, there has been a severe outcry regarding its use especially with regards to the implications it might have on privacy. With India on the verge of becoming a goliath in the world economy, it is also on its way of setting up the biggest facial recognition system in the world. In this article the author's seek to address the concerns regarding privacy while pin pointing lacunae in the existing legal regime and also suggesting recommendations with the intent that India's transition into a digital economy is a smooth one with minimal setbacks.

I. INTRODUCTION

Artificial Intelligence is the new revolution in the world of technology and its application is being seen in various fields. Everything in-between policing to decision making is being conducted through the mechanism of Artificial Intelligence Technology.

There is a growing concern surrounding the ethics behind the use of AI and its impact on our lives. We need to address such issues in order to be prepared for the future. Such advances are not only overwhelming but frightening at the same time and it is difficult people to maintain their pace with changes around the world. The following last couple of months has seen the use of Automated Facial Recognition Technology in India for the purpose of curtailing crime.

[1] Author is a student at National Law University and Judicial Academy, Assam, India.

[2] Co-Author is a student at National Law University and Judicial Academy, Assam, India.

The efficacy of the technology and research is very limited in India and that is the reason it is the right time to formulate a good strategy regarding the same. Further, we need proper accountability so that it does not see any form of misuse. This article deals with such issues and the need for India to lay a solid ground work so that problems do not arise in the future. The beginning of this article addresses the workings behind facial recognition technology, historical evolution and utility while warning the readers of the implications arising from the same.

The later sections of this article are dedicated to addressing the implications facial recognition technology might have on the right to privacy in India by firstly alluding the reader's attention to it being safeguarded as a Fundamental Right and then going about discussing existing lacunae's in India's data protection regime and finally ending with recommendations so that the interests of the state and industry are balanced while maintaining the right to privacy.

II. THE EVOLUTION OF FACIAL RECOGNITION TECHNOLOGY

The idea of identifying an individual suspected of having committed a crime is a concept that dates back to as early as the nineteenth century.[3] The focal point of having facial recognition technology (hereinafter referred to as FRT) is nothing but a linear progression of decade's worth of effort by law enforcement and governmental agencies trying to perfect the basic precept of photo identification.[4]

Although, the general public made wide use of it only when it came as a feature of unlocking one's iPhone, the efforts toward its development can be traced as far as the 1960's.[5] Back then, technology had begun developing that could identify pictures of individuals by manually inputting measurements of an individual's facial structure such as the eyes, nose, mouth and hairline.[6] FRT saw much progress in the 1980's when the process incorporated algebraic techniques which resulted in fewer than 100 measurements being needed to be taken in order to effectively code a face.[7] Finally in the 1990's, a massive expansion was seen when the Defence Advanced Research Products Agency ("DARPA") sponsored "FERET" or the 'FacE REcognition Technology Evaluation' so that it could be rolled into the

[3] Marcus Smith, Monique Mann & Gregor Urbas, Biometrics, Crime And Security 54 (Routledge 2018).

[4] *Id.*

[5] Kelly Gates, Our Biometric Future: Facial Recognition Technology And The
Culture Of Surveillance, 27, (New York University Press, 2011).

[6] JESSE D. WEST, *A Brief History of Face Recognition*, FACEFIRST (Aug. 1, 2017), https://www.facefirst.com/blog/brief-history-of-face-recognition-software.

[7] *Id.*

commercial market.[8] It is because of these efforts FRT can be seen being used widely in both the public as well as the private sector.[9]

In today's era, most FRT technology uses two fundamental processes, these are enrolment and matching.[10] In Algorithms, the face is divided into distinctive Nodal points. These points are different amongst different people and rarely see any change even if a considerable long period of time has passed.[11] FRT seeks out patterns by the use of features such a person's eye sockets, nose shape, weighted areas of the skin and also distances between unique features such as moles and spots.[12] This is known as the enrolment phase[13] and by its help it is used to create a digital "faceprint".[14] Thereafter, while identifying a person from another the said FRT software in question compares the data it is presently receiving to the already existent database filled with facial models, this is known as matching or verification.[15] The subsequent section will discuss how FRT is being employed by different countries and the growing concerns that are arising because of the same.

III. THE USES OF FRT AND GROWING CONCERNS ASSOCIATED WITH IT

In countries such as the U.S.A, F.R.T is being used in various sectors as a means of ensuring security and promoting safety.[16] It has wide range of uses such as in airports, it is being used as a way to combat passport fraud and it is also seeing use by the law enforcement agencies as a method to uncover the identity of missing children and a way to decrease identity fraud.[17] The most profound reason FRT is being used in the U.S is the occurrence of mass shootings which have arisen due to the expansion of gun culture due to the "right to bear arms" stated in the 2nd Amendment of the Constitution.[18]In the U.K, FRT technology is being used as a method of identifying persons visiting prisons. Even though it has been a subject matter of controversy amongst civil rights advocates, the programme has been successful in stopping drug smuggling amongst inmates.[19]

[8] *Id.*

[9] *Id.*

[10] Federal Bureau of Investigation, Subcommittee on Biometrics, Face Recognition 93 (2014). [hereinafter referred to as FBI Biometrics]

[11] SMITH et al., *supra* note 1, at 7.

[12] SHARON NAKAR & DOV GREENBAUM, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, B.U. J. SCI. & TECH. L.88, 95 (2017).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] JESSE D. WEST, *supra* note 4.

[17] FBI BIOMETRICS, *supra* note 8.

[18] U.S CONST. Amend. II.

[19] *Prisons are using face recognition on visitors to prevent drug smuggling*, MIT TECHNOLOGY REVIEW,

An important application of FRT is that it is also used a means of verification and identification in schools.[20] The reason being cited is for security related concerns.[21] However, the technology has seen an expanded use in China where it is being used to monitor how attentive children are in the classroom.[22] The system determines whether children are focused on their lessons by identifying facial expressions through the use of cameras which are installed above blackboards. The teachers then evaluate such information to give them grades.[23]Alarmingly, China is not alone as the use of the technology for the same purpose is contemplated even in the West. At North Carolina University, researchers have recorded the faces of students in a similar way to assess whether they were having trouble understanding the material they were being taught.[24] Also, at New York, a company called 'SensorStar Labs' is monitoring children using a facial software called 'EngageSense'. It makes the use of algorithms to interpret the level of engagement shown by the students.[25] This could be soon started to monitor students' performance.[26]

The use of FRT has seen an increased growth in the private sector as well.[27] Major retailers and venues have begun using these technologies to detect shoplifters, monitor crowds, and even scan for unhappy customers.[28]In China, the rapid development of the technology has seen its application in the form of facial payment (hereinafter referred to as FP). FP gives consumers an option of hassle free payment once they sync their facial information with their accounts.[29] Applications such as Alipay and WeChat have powered the trend of its use in

(Mar. 6, 2019) https://www.technologyreview.com/the-download/613080/prisons-are-using-facerecognition-on-visitors-to prevent-drugsmuggling/.

[20] SMITH et al., *supra* note 1, at 56.

[21] AVA KOFMAN, *Face Recognition is Now Being Used in Schools, but It Won't Stop Mass Shootings*, THE INTERCEPT (May 30, 2018, 10:06 P.M.), https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/.

[22] XINMEI SHEN, *China is Putting Surveillance Cameras in Plenty of Schools*, TECH IN ASIA (Jan. 22, 2019), https://www.techinasia.com/china-puttingsurveillance- cameras-plenty-schools.

[23] RACHEL ENGLAND, *Chinese School Uses Facial Recognition to Make Kids Pay Attention*, ENGADGET (May 17, 2018), https://www.engadget.com/2018/05/17/chinese-school-facial-recognition-kidsattention/.

[24]KECIA LYNN, *Bringing Facial Recognition Software into the Classroom*, BIG THINK (July 1, 2013), https://bigthink.com/ideafeed/bringing-facial-recognitionsoftware-into-the-classroom.

[25] RANDY RIELAND, *Can Facial Recognition Really Tell If a Kid Is Learning in Class?,* SMITHSONIAN MAG. (Nov. 1, 2013).

[26] ROBERT D. BICKEL, *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in A Democracy, or Will the Courts Strike A Proper Balance?*, 33 STETSON L. REV. 299, 305 (2003) (discussing how security cameras can also be used to monitor workplace performance).

[27] JENNA BITAR & JAY STANLEY, *"Are Stores You Shop at Secretly Using Face Recognition on You?, "American Civil Liberties Union*, ACLU, (Mar. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillancetechnologies/are-stores-you-shop-secretly-using-face.

[28] JOHN BRANDON, *Walmart Will Scan for Unhappy Shoppers Using Facial Recognition (Cue the Apocalypse),* VENTUREBEAT, (Aug. 9, 2017), https://venturebeat.com/2017/08/09/walmart-will-scan-for-unhappy-shoppers-using-facial-recognition-cue-the-apocalypse/.

[29] LI CHENGLONG, LI HONGXIU & WANG PING, *Facial Payment Use in China: An Integrated View of*

dozens of cities.[30]

Thus, the technology certainly comes with many hurdles that need overcoming. Its use is questionable as there is evidence to suggest that FRT is susceptible to error particularly while used for identifying African Americans, ethnic minorities, women and young people.[31] A testament to this was when Amazon's REKognition incorrectly identified 28 members of the Congress as having been arrested for crimes. The false matches were disproportionately people of colour.[32] Similarly, on testing Microsoft and IBM's face analysis software's it was determined that they were excellent at identifying white males but less accurate when it came to identifying people with black skin.[33]

Another alarming implication is that it will normalize invasive means of surveillance in the eyes of students at a very young age.[34] This would result in immense ramifications on the way students perceive the government's place in monitoring behaviour in the interest of safety.[35] Students may come to think that cameras have the capability to recognize who they are and are specifically used to track them to ensure obedience.[36] The learning environment will become less nurturing which is crucial in imparting a proper education. [37]It might also lead to heightened penalization of minor offences which would normally go unnoticed.[38]Such an idea is antithetical and subversive to the entire notion of liberty where an individual's civil and political rights are of prime importance. Lastly, in case FRT being employed for FP, there have been concerns that the biometric information that has been collected could be stolen and misused by hackers.[39]However, the crucial area of this research is regarding the implications of privacy due to FRT. The subsequent section will see the author's elucidating

Privacy Concerns and Perceived Benefits, PACIS 2020 Proceedings 68, 68 (2020), https://aisel.aisnet.org/pacis2020/68

[30] *Id.*

[31] ROSARIO GIRASA, ARTIFICIAL INTELLIGENCE AS A DISRUPTIVE TECHNOLOGY – ECONOMIC TRANSFORMATION AND GOVERNMENT REGULATION 115 (Palgrave Macmillan, 2019).

[32] RACHEL METZ, *Amazon investors want it to quit selling facial recognition tech to the government*, CNN BUSINESS, (Jan. 17, 2019). https://www.kmov.com/news/amazon-investors-want-itto-quit-selling-facial-recognition-tech/article_2cdff0ec-6baa-536f-ba5c-1b09e7b28e27.html.

[33] DAVID RAND, *Facial recognition can drive business goals, but where do we draw the line?* HEWLETTPACKARD ENTERPRISE (Feb. 25, 2019), https://www.hpe.com/us/en/insights/articles/facial-recognition-can-drive-business-goals-but-where-do-we-draw-the-line-1902.html, quoting Gartner.

[34] J. WILLIAM TUCKER & AMELIA VANCE, *School Surveillance; The Consequences for Equity and Privacy*, 2 EDUCATION LEADERS REPORT 4, 3 (Oct. 2016) (citing a report conducted by the U.S. DEPARTMENT OF EDUCATION, NATIONAL CENTER FOR EDUCATION STATISTICS, PUBLIC SCHOOL SAFETY AND DISCIPLINE: 2013-2014 (2015)).

[35] *Id.*

[36] TUCKER & VANCE, *supra* note 32, at 9.

[37] *Id.*, at 8.

[38] *Id.*, at 12.

[39] LI CHENGLONG et al., *supra* note 27.

privacy as a concept and the constitutional safeguards that protect it as a Fundamental Right in India.

IV. Privacy and its relation to the ongoing use of FRT in India

Privacy is the right to be left alone.[40] Aristotle the Greek philosopher spoke of a division between the public and private sphere.[41] His distinction formed a basis to confine government authorities to activities carried out in the public realm whereas, activities in the private realm were to be excluded.[42]

A wider connotation was given by Austin in his lectures on Jurisprudence where he spoke of the distinction between public and private realms. He believed the rationale of privacy does not cease only because the said person has to interact with others in a public arena. There might be a difference between the extents to which an individual expects privacy at home compared to what he does in the streets, yet, if dignity is the basis of recognizing privacy the right is not controverted merely on such basis.[43]

Later, Samuel D Warren and Louis Brandeis in their article published in Harvard Law Review discerned the impact technological progress could have on the right to privacy.

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons…

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by

[40] DOROTHY J GLANCY, *The Invention of the Right to Privacy*, 21 A.L.R 1, 2-3 (1979) "The article attributes the Roscoe Pound quotation to "Letter from Roscoe Pound to William Chilton (1916)" as quoted in Alpheus Mason, *Brandeis : A Free Man's Life* 70 (1956)" .

[41] MICHAEL C. JAMES, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 21(2) C J I L 252, 261 (2014).

[42] *Id.*, at page 262

[43] Justice K.S.Puttaswamy (Retired). v. Union of India And Ors. (2017) 10 SCC 1 (India).

mere bodily injury."[44]

The technology which propelled the authors to write the said article was the development of photography. However, the ringing observations bear crucial significance today in a world enveloped by the Internet where technology like FRT is seeing prolific use.

Today, numerous international covenants give recognition privacy as a specific right. These include the UDHR[45], ICCPR[46], the U.N Convention on Migrant workers[47] and the UNCRC[48]. The same can be said about various treaties at a regional level such the 1950 Convention for the Protection of Human Rights[49].

In India, the right to privacy has been accorded the status of a Fundamental Right after the seminal judgement provided by the Supreme Court in the case of *K.S Puttaswamy v. Union of India*[50]. It was ruled by a nine judge bench where Justice D.Y Chandrachud writing a multiplicity judgement observed that privacy is a constitutionally protected right which emerges from the guarantee of life and personal liberty accorded in Article 21 of the Constitution[51]. It is a constitutional core of human dignity and elements of Privacy also arise in varying contexts from the facets of freedom and dignity recognised and guaranteed in Part III.[52] While the expectations of privacy may vary between public and private arenas, it is important to underscore that privacy cannot be lost or surrendered merely because the individual is in a public place.[53]It also warned about how technological change has given rise to concerns which were not present a few decades ago and that rapid growth of technology may render void many notions of the present.[54] In case there arises a situation where privacy must be curtailed, the law which encroaches upon privacy must be fair, just and reasonable[55]. Legitimate aims of the State giving rise to such include instances such as national security, preventing and investigation of crimes, encouraging innovation and dissipation of knowledge and preventing the unjust distribution of social benefits. Due regard of what has been

[44] WARREN & BRANDEIS, *The Right to Privacy*, 4(5) H. L. R. 174, 193.
[45] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A (III).
[46] International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.
[47] UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, A/RES/45/158.
[48]UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series, vol. 157.
[49] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.
[50] Justice K.S.Puttaswamy (Retired). v. Union of India And Ors. (2017) 10 SCC 1 (India).
[51] INDIA CONST. art 21.
[52] Justice K.S.Puttaswamy (Retired). v. Union of India And Ors. (2017) 10 SCC 1 (India).
[53] *Id.*
[54] *Id.*
[55] *Id.*

discussed in this judgements should be considered[56]

Presently, the government is making preparations to install a nationwide facial recognition system. India's National Crime Records Bureau which runs its operations under the Home Ministry has started to gather bids from private companies. The reason cited is that the technology will assist the police force in the country which is currently understaffed.[57] The tender mentions that the system will bring a monumental change in investigating crimes/handling of criminals/operations related to them by allowing security forces across India to access a centralised database of images.[58] Images will be pulled from newspapers, CCTV cameras, photographs used in passports, and social media accounts. It is however unclear who will be given the responsibility of operating this system and who shall be made accountable if something goes wrong.[59]

On the 23rd of February, 2020 riots erupted in East Delhi after supporters of the Bharatiya Janata Party clashed with those protesting against the Citizenship Amendment Act.[60] The aftermath saw devastating effects as it resulted in deaths and injuries of many people along with damage to households, shops and places of worship. After the riots had ended, Union Minister Amit Shah reported that 1,100 persons were identified using FRT who would be held accountable for the violence that had disrupted. Shah's announcements can certainly be seen as an overestimate to the capabilities of FRT as it has proved to be an unreliable method of identifying people especially those in crowds.[61] The technology also saw use in Uttar Pradesh where it helped detain a handful of more than 1,100 people who had alleged links to the violence that erupted during the protests in the state. [62]

More recently, amidst the Covid19 crisis, the Telengana Police have been heavily relying on FRT to ensure that those out on the streets are adhering to the social distancing protocols.[63] Gurugram is also ensuring that prison inmates are obeying social distancing norms by using a

[56] *Id.*

[57] VASUDEVAN SRIDHARAN, *India setting up world's biggest facial recognition system*, DW (Nov.7, 2019), https://www.dw.com/en/india-setting-up-worlds-biggest-facial-recognition-system/a-51147243.

[58] *Id.*

[59] *Id.*

[60] VAPALA BALACHANDRAN, *India's adoption of facial recognition technology could have serious ramifications*, ATLANTIC COUNCIL (Apr. 10, 2020), https://www.atlanticcouncil.org/blogs/new-atlanticist/indias-adoption-of-facial-recognition-technology-could-have-serious-ramifications/.

[61] *Id.*

[62] ALEXANDER ULMER & ZEBA SIDDIQUI, *India's use of facial recognition tech during protests causes stir*, REUTERS, (Feb.7, 2020, 4: 15 P.M.), https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ.

[63] ANEESHA BEDI, *Geo-mapping, CCTV cameras, AI — how Telangana Police is using tech to enforce Covid safety*, THEPRINT, (June 2, 2020, 5:30 P.M.), https://theprint.in/india/geo-mapping-cctv-cameras-ai-how-telangana-police-is-using-tech-to-enforce-covid-safety/433856/.

tool developed by 'Staqu technologies' which scans CCTV footage and alerts authorities in case of violations.[64]

In the absence of any specific laws which can effectively regulate and provide specific guidelines for the use of FRT, its use has become a cause of growing concern. India might soon be submitting to a regime where the State keeps constant vigilance on everything that is happening without check. Keeping in line with what was discussed in the Puttaswamy judgement the government should enact legislation in order to ensure that the right to privacy is properly safeguarded while supporting legitimate interests of the State. If the same is done it will provide clarity regarding the extent and conditions in which FRT may be used. The subsequent section will showcase how far India has come along in the process of legislating laws governing FRT and other AI.

V. THE KEY ISSUES CONCERNING EXISTING LEGISLATION

In presence of great power, great responsibility follows it too. A.I under whose ambit FRT falls vests great amounts of power on the State. Thus, it has responsibility to protect its citizen's privacy and hold accountability in case of infringement of such rights. AI bears great implications and has many legal issues.

If we look at the current scenario in India, we can see that regulation of personal data is being done through the Information technology (IT) Rules, 2011 under the IT Act, 2000[65]. Rule 3 of the act[66] categorizes items which can come under the purview of sensitive information. It also incorporates the policy for disclosure of information and privacy[67]. There should be proper reason for collection of Sensitive Information and accountability is there to ensure protection against the misuse of Information. The rules basically hold companies accountable in case there is threat to the security of the personal data of a person[68]. The IT act is a good attempt to protect the data and to ensure that reasonable and fair practices regarding handling of the same but development of technology is happening rapidly. The definition of sensitive data is quite narrow and the Act is only for holding companies liable. There is no inclusion of the State.

[64] ANU THOMAS, *As IBM Exits Facial Recognition Business, A Look At How The Tech Has Advanced In India,* ANALYTICSINDIAMAG, (June 9, 2020), https://analyticsindiamag.com/as-ibm-exits-facial-recognition-business-a-look-at-how-the-tech-has-advanced-in-india/.

[65] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (India).

[66] The Information Technology Act, (21 of 2000) 2000 (India).

[67] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, Rule 7, 2011 (India).

[68] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, Rule 3, 2011 (India).

Today, AI is mostly dependent upon big data which is fed to machines which reaches a conclusion regarding that same. For instance, Aadhar Card information is stored in big databases[69] and FRT will use this data to catch criminals[70] or identify missing children. Data protection laws have started evolving after the Puttaswamy precedent[71] which renders privacy as the fundamental right of the people.

The Personal Data Protection bill was developed on the lines of report submitted by Retired Justice B.N. Srikrishna committee[72]. This bill put India on the forefront for developing its own legislation regarding data protection and ensuring fair and safe use of the personal data of an individual. It regulates data collected by the companies, Government and foreign companies in order to give rights to individuals over their personal data.[73] NITI Aayog, in its 2018 report said that India is going to have seven hundred and thirty million users by 2020[74] and the amount of data people share on Internet can be used by companies in order to have an edge in business violating provisions of competition law[75]. Use of data should always be for fair purposes and at the choice of an individual to give their data away. The bill of 2019 has several lacunae as the proposed law draws foggy distinction between personal and non-personal data. Legislation should be drafted keeping the future in mind as it will be useful when there will be advancement of AI and Machine learning. All of the data according to the current bill is being regulated by the agencies of the State. It does not give any mechanism through which there will be checks and balances except one or two cases. It is really important that the citizens of the country can understand the principle behind such law and how it’s being regulated.

The most controversial aspect the data bill is the localization of data[76], it makes mandatory for firms and companies to have at least one serving copy of their personal data in the databases located in India. This clause of the bill also declares certain area of data as critical and such data can only be stored in India. The only reason to have personal data in the

[69] MADHAV KHOSLA & ANANTH PADMANABHAN, *The Aadhaar Challenge: 3 Features That Put Constitutional Rights at Risk*, THEPRINT, (June 27, 2018), https://theprint.in/opinion/the-aadhaar-challenge-3-features-that-put-constitutional-rights-at-risk/75576/.

[70] Information Technology Act, Section 69, (21 of 2000) 2000 (India).

[71] Justice K.S.Puttaswamy (Retired). v. Union of India And Ors. (2017) 10 SCC 1 (India).

[72] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, “Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna,” Committee Report (India: Ministry of Electronics & Information Technology, Government of India, Jul. 27, 2018).

[73] Personal Data Protection Bill, No. 373 of 2019, Clause 14, 2019 (India).

[74] Indian telecom services performance indicators, Telecom Regulatory Authority of India, December 2013 and June 2017; calculated as number of subscriptions divided by total population, World Bank, April 19, 2018. 44 Strategy Analytics, May 2017.

[75] RICHARD WHISH & DAVID BAILEY, COMPETITION LAW 603, (Oxford University Press, 2015).

[76] Personal Data Protection Bill, No. 373 0f 2019, Clause 33, 2019 (India).

databases located in India would be for authorities to have it at their fingertips. According to the bill, by procedure established by law, state can access the personal data for detection, investigation or any other contravention of law under an umbrella of national security. This section allows the state to have access to great amount of personal data of users and this data can be used for various purposes and is a threat to the right of users to their privacy.

The regulatory structure of this is not independent and the government at the center has most of the control over this regulatory regime. This Bill is a halfhearted attempt to regulate privacy laws and something needs to be thought up for the long run to cater to rapid advancement of AI. The next section will discuss recommendations to see improvements.

VI. CONCLUSION AND RECOMMENDATIONS

Today AI is deployed rapidly despite many ethical concerns being present. It is being used across multiple sectors and forms the major part of our lives. There is no legislation to regulate AI and its surveillance through FRT in India. Below are recommendations provided by the author's to improve the situation.

- Formulating data protection law which can serve the needs of a futuristic digital industry. Though Personal Data Protection Bill is still under the process to become a law, it needs to address major privacy concerns of users and to provide safety net for the user regarding access of their data by the government.
- Disbanding the use of FRT until there is proper development and adequate research conducted to place regulations: Artificial Intelligence and facial recognition technology should not be deployed at places where decision making power of the software affect human lives. For instance, if FRT misinterprets the face of the accused and matches it with some other person then it will cause severe impact on the life of an individual. Thus, use of FRT and AI should be researched and then this data should be used to decide whether we can deploy such technology in our lives.
- India can take lessons from other countries: China and United states are leading the world in the research related to the Artificial Intelligence. The U.S uses billions to fund the research and development of the Artificial Intelligence but most of its market is driven by key private players like Microsoft, IBM, Apple, etc. This shows that investment in public sector drives the private market. U.S and China have structure with proper governance and clear goals regarding AI usage. Investors drive the market and hence, help in the research and development of the sector which results in

better economy and growth. There should be collaboration and interdisciplinary approach in order to boost the sector.

- India should meet International standards for law related to Data protection and privacy: In May 2018, Important Guidelines of European Union’s General Data Protection Regulation was published and encouraged of framework which is less invasive in nature in terms of privacy. France went ahead a step further by giving framework which explains algorithmic decisions taken by the software. Laws in India need to be framed which will help in understanding the impact and risks coming up with the application of such technology and making it part of our lives.

We know that FRT systems are prone to privacy concerns. Yet, huge capital is being investing in it which will cause major impact on our lives and result in lot of challenges. A lot of steps need to be climbed for the bright and healthy future of our country while FRT exists.

*****