ARTIFICIAL INTELLIGENCE: A THREAT TO PRIVACY?

Dr. Sunitha Abhay Jain*
Ms. Simran A. Jain**

ABSTRACT

Klaus Schwab has observed that, "The Fourth Industrial Revolution, finally, will change not only what we do but also who we are. It will affect our identity and all the issues associated with it: our sense of privacy, our notions of ownership, our consumption patterns, the time we devote to work and leisure, and how we develop our careers, cultivate our skills, meet people, and nurture relationships."[1] *Advances in Artificial intelligence have transformed our world. John McCarthy from the Computer Science Department of Stanford University coined the termand defined it as, the science and engineering of making intelligent machines.*[2] *Artificial intelligence is where a machine possesses the intelligence as that of a human being. Such machines with artificial intelligence, like anyother human being can react to and contemplate the environment it is in and react accordingly. It collects information around it and has the ability to take decisions accordingly. This system of artificial intelligence though sounds helpful on prima facie understanding; it has been a threat to the*

** Associate Professor; LLM Co-ordinator, School of Law, CHRIST (Deemed to be University), Bangalore.The author can be reached at sunitha.abhay@christuniversity.in*

*** Gujarat National Law University, Gandhinagar, Ahmedabad. The author can be reached at simijain18@gmail.com*

[1] http://www.journals.ac.za/index.php/sajhe/article/download/633/248

[2] http://www-formal.stanford.edu/jmc/whatisai.pdf

privacy of an individual. These artificial intelligence mechanisms are controlled by softwares which are developed by human entities. Such owners have a control over the action and reaction of the artificial intelligence mechanism. In today's digitalised world every individual in one or the other way is subject to the use of technology. Enormous amount of personal data is stored as digital data, which the artificial intelligence mechanism is making use of, in view of the betterment of standard of living. On the flip side, all personal data including our finger prints, travel details, frequent interaction with a particular persons, medical reports are collected, stored, processed, profiled with the help of Artificial Intelligence. This invades a person's privacy.

In this background, the paper tries to analyze the invasion of privacy by Artificial Intelligence and the ill-effects of the same. In the guise of public good even the government has adopted AI mechanisms which lead to questioning the governmental action. Likewise, there is hardly any legislation that regulates these aspects either on the national or on the international platform. The paper focuses on India and lack of any legislation till date to protect an individual's Privacy. Since the Supreme Court of India has upheld that right to privacy is a fundamental right under Article 21 of the Constitution of India, though not an absolute right, it is high time a comprehensive Privacy legislation is enacted in India.

Keywords*: Artificial Intelligence; Right to Privacy; Data Protection; Human Rights.*

I. INTRODUCTION

With the technological revolution and especially the use of Artificial intelligence, our lives have been transformed in a manner that was never perceived or fathomed before. With the advent of Artificial Intelligence, the intelligent machines enable high-level cognitive processes like thinking, perceiving, learning, problem-solving and decision-making, coupled with advances in data collection and aggregation, analytics and computer processing power.[3] These technological innovations have become ubiquitous and all pervasive, touching every sphere of our lives. We are witnessing a fourth revolution which has created a '*technomy community*'.[4]Schwab has observed that,"*we are on the threshold of a technological revolution which will alter the way we live, work and relate to one another. In its scale, scope and complexity, the transformation will be unlike anything humankind has experienced before. We do not yet know just how it will unfold, but one thing is clear: the response to it must be integrated and comprehensive, involving all stakeholders of the global polity, from the public and private sector to academic and civil society.*"[5]The fourth Industrial revolution is characterized by the convergence of various technologies such as data analytics, artificial intelligence, cognitive technologies and internet of things.[6]It has been observed by Brian Householder[7] that, "*The concept of digitizing everything is becoming a reality. Automation, Artificial intelligence, Internet of things, machine learning and other advanced technologies can quickly capture and analyze a wealth of data that gives us previously unimaginable amounts and types of information to work from. Our challenge becomes moving to the next phase-changing how we think, train and work using data-to create value from the findings obtained through the advanced technologies.*"[8]

Artificial Intelligence revolution is emerging at a fast pace in India and as it has the potential to transform the economy there is an urgent need for the Indian Government to strategize for development of Artificial Intelligence. The Hon'ble Finance Minister has taken a step in the right direction when he

[3] http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

[4] https://www.ey.com/Publication/vwLUAssets/ey-future-of-jobs-and-its-implication/$File/ey-future-of-jobs-and-its-implication.pdf

[5] Xu, Min & M. David, Jeanne & Hi Kim, Suk. (2018).,*The Fourth Industrial Revolution: Opportunities and Challenges*, International Journal of Financial Research. 9. 90. 10.5430/ijfr.v9n2p90.

[6] https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/gx-fourth-industrial-revolution.pdf

[7] President and Chief Operating Officer, Hitachi Vantara

[8] https://www.forbes.com/forbes-insights/wp-content/uploads/2018/01/Deloitte-FourthIndustrialRev_REPORT_FINAL-WEB.pdf

mandated the NITI Aayog to establish the National Program on AI in order to usher in the research and development in the field of AI.

II. ARTIFICIAL INTELLIGENCE

The idea of computer based artificial intelligence came to fore with Alan Turing's test which inquires into the question as to whether a computer can think like a human being. The first artificial neural network was built a few months later by Princeton students. The term, 'Artificial Intelligence' was coined by Mr. John Mc Carthy and defined it as, "the science and engineering of making intelligent machines."[9] The first AI program, 'Logic Theorist' was developed by researchers at the Carnegie Institute of Technology. In MIT an Artificial Intelligence Laboratory was founded by Marvin Lee Minsky. Much advancement was made in Cambridge to develop semantic networks for machine translation and also to develop self learning softwares at IBM. The interest in AI emerged again in the recent years as there are many advances in the field of deep learning, faster computers and more data which has convinced the investors that it is viable and profitable to work with Artificial Intelligence. Billions of dollars are being invested by Tech giants like Amazon, Apple and Google in various technologies for the development of Artificial Intelligence.

The tasks associated with intelligent humans when performed by digital computer or robots is termed as Artificial Intelligence. Many aspects of our lives have been touched by Artificial intelligence. Many sectors like transportation, health care, education, entertainment industries are using AI to carry out the work. Medical care and research is undergoing a sea change with the use of Machine learning algorithms. In order to identify high impact molecules for drug development and to accelerate skin cancer diagnosis these technologies are being used. A recent report by Mc Kinsey found that 45% of all work activities could soon be automated using AI.[10]

[9] http://www-formal.stanford.edu/jmc/whatisai.pdf

[10] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet

III. CONCEPT OF PRIVACY

The concept of Privacy is not a new one and one can find references to it since times immemorial. The early references to privacy violation and protection can be found in the passages of bible. Any person who violated or intruded into someone's private life was viewed with anger and shame. The Code of Hammurabi also mentioned against intrusion into someone's home. Right to Privacy was protected in the Hebrew culture, ancient Greece and China.

It is very difficult to define the term '*privacy'* as the meaning varies according to the context, environment and from society to society. Privacy is sometimes fused with Data protection in some countries to mean protection of personal information.

Privacy has various facets such as Information privacy; bodily privacy; privacy of communications and territorial privacy. Information privacy refers to the protection of personal information or data like the credit card details, health information etc. The protection to the physical selves of people against invasive procedures like testing of drugs, cavity searches falls within the purview of bodily privacy. Further, privacy can also be understood to mean the privacy of communication which includes the security and privacy of mails, telephones, emails and any other form of communication. Territorial privacy refers to setting of limits into one's domestic or other spheres like one's workplace or public space.[11]

The idea of privacy stems from distinguishing between what is '*Private*' and '*Public*'which helps in drawing limits between 'oneself' and the 'outer world'. The concept of privacy was articulated by Justice Louis Brandeis when he referred to privacy as the right of an individual,'*to be left alone*'which ensured protection against the unwanted disclosure of private facts, thoughts, emotions etc.[12]Alan Westin,in his the seminal work 'Privacy and

[11] http://gilc.org/privacy/survey/intro.html

[12] http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

Freedom 'emphasized upon the fact that privacy includes the choice of people to determine the extent to which they will expose themselves, their attitudes and their behavior to others.Privacy has also been described as a quasi'*aura*' around the individual, whichconstitutes the limit between him/her and the outside world. Privacy has different facets like the right to be let alone; limited access to the self; secrecy; control of personal information; personhood and intimacy.[13]According to Ruth Gavison, *Secrecy*, *Anonymity* and *Solitude* are the three elements of privacy. Privacy can be lost when a person chooses to do so or it can also be lost through the action of another person.[14]Richard Posner, an American jurist and economist refers to privacy in terms of withholding and concealment of information.[15]Westin is of the view that privacy is the claim of an individual to determine what informationabout himself, he wants to share with the others. Fried defines Privacyin terms of the control that one can have over the information about oneself.[16]According to American Edward Blousteinwhen there is an intrusion into privacy of a person it has some connection with the'*personhood, individuality andhuman dignity'*of that individual.[17]Tom Gerety, an American Professor terms privacy as "the control overor the autonomy of the intimacies of personal identity."[18] Hungarian Jurist Máté Dániel Szabó,argues the right of an individual to decide about himself or herself can be termed as 'privacy'."[19]

IV. INTERNATIONAL FRAMEWORK FOR PROTECTION OF PRIVACY

Human rights form the cornerstone of any civilised society. The right to privacy has been categorised as a first generation human right. Privacy is a

[13] https://pdfs.semanticscholar.org/b4dd/520e60148e04ae22d2fc33415398e0736fff.pdf
[14] Supra n. 9
[15] https://www.passeidireto.com/arquivo/49651384/what-is-privacy—the-history-and-definition-of-privacy—adrienn-lukacs/2
[16] ibid
[17] ibid
[18] ibid
[19] ibid

fundamental human right recognized in the Universal Declaration of Human Rights, 1948 (Article 12)[20]and the International Covenant on Civil and Political Rights,1966 (Article 17);[21] Convention on the Rights of the Child,1990(Art.16); [22]and International Convention on the Protection of all Migrant workers and members of their families, 1990(Art.14).[23]The right to privacy is protected at the regional level under the European Convention for the protection of Human rights and fundamental freedoms(Art.8);[24]and American Convention on Human rights, 1969(Art.11)[25] amongst others. Cairo declaration on human rights in Islam, 1990 (Art.18)[26]; Arab Charter on human rights,1994 (Art.16 and 21)[27]; African charter on the rights and welfare of the child (Art.19)[28];Asia-pacific economic cooperation privacy framework[29]; Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data,1981[30]; Additional Protocol to the Convention for the Protection of individuals with regard to personal data regarding supervisory authorities and trans-border data flows, 2001[31]; European Union Data Protection directive [32] also protect privacy rights.

Most of the countries of the world have recognized the right to privacy in their Constitution. During this time, the inviolability of the home and secrecy

[20] http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

[21] https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

[22] https://www.ohchr.org/documents/professionalinterest/crc.pdf

[23] https://www.ohchr.org/en/professionalinterest/pages/cmw.aspx

[24] https://www.echr.coe.int/Documents/Convention_ENG.pdf

[25] https://www.cartercenter.org/resources/pdfs/peace/democracy/des/amer_conv_human_rights.pdf

[26] http://www.bahaistudies.net/neurelitism/library/Cairo_Declaration_on_Human_Rights_in_Islam.pdf

[27] http://www.humanrights.se/wp-content/uploads/2012/01/Arab-Charter-on-Human-Rights.pdf

[28] https://au.int/sites/default/files/treaties/7773-treaty-0014_ _african_charter_on_the_rights_and_welfare_of_the_child_e.pdf

[29] https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

[30] https://rm.coe.int/1680078b37

[31] https://rm.coe.int/1680080626

[32] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

of communication were protected by most of these provisions.Some countries like South Africa and Hungary have included right to access and control one's personal information.However countries like the United States of America, Ireland have not explicitly recognized privacy in their Constitution. Countries around the world have worked around adopting comprehensive privacy laws and many of the laws are based on themodels adopted by the OECD and the Council of Europe. European Union directive lays emphasis on the protection of personal data which has set a benchmark for national laws. Countries outside Europe Union have drawn inspiration from this and have passed privacy laws. Many countries are in the process of enacting data protection laws and more than forty countries have already enacted data protection or information privacy laws.

V. RIGHT TO PRIVACY: AN INDIAN PERSPECTIVE

Nariman J. traced the constitutional foundations of privacy to the Preamble stating as follows: "The dignity of the individual encompasses the right of the individual to develop to the full extent of his potential. And this development can only be if an individual has autonomy over fundamental choices and control over dissemination of personal information which may be infringed through an unauthorized use of such information.[33]

Right to Privacy is not specifically guaranteed under the Constitution of India but has been interpreted by the courts to be protected under Art.21 of the Constitution. The right to privacy is not an absolute right but can be subject to reasonable restrictions in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.[34] The Supreme Court's decision in the case of Justice K.S. Puttaswamy (Retd) v. Union of India[35] is a resounding

[33] https://indconlawphil.wordpress.com/2017/08/."

[34] Article 19(2) of the Constitution of India, 1950

[35] https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

victory to the right of Privacy.In this case the constitutional validity of the Indian biometric identity scheme Aadhaar was challenged. This is considered to be a watershed moment in the constitutional history of India as the right to privacy has been endorsed by the highest court of the country. All the nine judges unanimously agreed that, the *right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.*[36]

There is a void in the Indian legal system as far as data protection is concerned as Indiadoes not have comprehensive data protection legislation in place. India is contemplating to enact privacy legislation with efforts being made in this direction with an Approach Paper on Privacy and the Report of the Group Experts on Privacy. The personal information is afforded legal protection in India under Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Section 43 A of the Information Technology Act mandates reasonable security practices to be maintained by body corporate if it receives, possesses, deals, or handles any 'sensitive personal data'. Any failure on their part to do so will result in liability and the corporate will have to compensate for the loss suffered.[37] Today the Government authorities and other non-governmental bodies initiatives are data driven. For instance, the Unique Identity scheme, National population register collect vast amount of personal data of individuals. Further many e-government projects rely on vast amounts of data which further adds to the problem of data protection and raises privacy concerns. However, Section 43A of the Information Technology Act, 2000 is lacking as far as protection of data is concerned in the public sectors. The scope of protection afforded under it is limited to personal and sensitive data. The problem is further aggravated as usually

[36] https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time

[37] https://indiacode.nic.in/handle/123456789/1362//simple-search?page-token=437d9d6bd053&page-token-value=fa92e035a6f1a6271abe3958ebe97eae&nccharset=29BF10FA&query=information+technology+Act%2C+2000

data is of dynamic nature and due to generation of new forms of data and data sources and the evolving nature of data, the protection afforded under Section 43A falls short. Further, the definition of personal sensitive data is also limited. Personal information is defined to mean any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 defines "sensitive personal data or information" to include password; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information. It is necessary that certain kinds of personal information are particularly sensitive due to the intimate nature of their content and need to be protected. However, this definition is inadequate as it does not include electronic communications such as emails, browsing and chat logs within its scope. The consent of the data subject needs to be taken in writing before the collection of sensitive personal data.[38] The data collectors must ensure that the consent is informed and freely given. The application of consent before the collection of personal data is significantly narrowed by the fact that the Rule 5 applies only to sensitive personal data or information and not all kinds of personally identifiable information.[39] Thus it can be seen that Section 43A of the IT Act and the 2011 rules do provide for many similar provisions as under the General Data Protection Regulation (GDPR) but applicable only for residents of India.

The European Union has enacted the EU GDPR, which replaces the Data Protection Directive of 1995 and has come into force on 25th May 2018. It is a

[38] Rule 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

[39] https://privacyinternational.org/sites/default/files/201804/India_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf

comprehensive legislation that deals with all kinds of processing of personal data. It also lays down the rights and obligations of parties. It lays down the fundamental norms for the privacy protection of the Europeans. GDPR will be applicable not only for EU companies, but alsoto many third world countries including India. Companies that deal with the data of the EU residents or if they are providing any goods and services which involves handling of data or if they monitoring or profiling data of EU people they are required to comply with the GDPR. Compliance with the GDPR has become a major cause of concern for the Multinational companies as the GDPR is having far reaching effects in the international arena and the penalties provided under GDPR are very hefty. Under the GDPR restrictions can be imposed on the basis of meeting the 'adequacy requirement' which basically means restrictions on the transfer of data to any other country or organization of international nature which donot have adequate level of protection in their country.In order to keep up with the changing landscape of privacy protection at the international level, it becomes imperative for the Indian Government to enact a privacy legislation.

There was a ray of hope for privacy protection when the Justice Sri Krishna Committee submitted the draft Personal Data Protection Bill, 2018. The bill gave importance to the consent of individual for the purpose of sharing of data. If personal data had to be shared or processed express consent of data subject had to be taken. To make an informed choice the burden fell on the data subject.The personal data must be processed in a fair and reasonable manner. Any failure on the part of the companies would attract penalties that can go up to Rs.15 crores or 4% of a company's turnover world over. The bill however does not address the issue pertaining to the ownership of the data. The Telecom Regulatory Authority of India had stated that each user ownshis data and the entities that are in the possession of data are mere custodians.Data is not treated as a 'property'but is treated as a matter of 'trust.'The consumers have the right to demand the deletion of their past record. Under the GDPR, the data subject could also exercise their 'right to be forgotten' which is defined as the right to restrict or prevent continuing disclosure of personal data. However the process of justifying why the consumer does not want to continue giving consent is also long drawn.[40]

VI. HOW ARTIFICIAL INTELLIGENCE CAN COMPROMISE ON OUR PRIVACY?

The emergence of increasingly sophisticated Artificial Intelligent systems and the convergence of many technologies like the Artificial Intelligence, the Internet of Things (IoT), and the related Internet of Living Things (IoLT) poses a serious threat to our privacy and security. The generation, collection, processing and sharing large amounts of data about an individual and collective behavior can be done with the help of Artificial Intelligence. One can analyze and optimize sensory data like the images of face, voice recording,vitals, DNA of an individual much faster and better than human beings with the help of Artificial Intelligence and by using computational algorithms enhanced with machine leaning capabilities. Inspite of various privacy and security issues associated with Artificial Intelligence countries and governments around the world are investing and developing Artificial intelligence technologies.The interconnectivity of AI systems which optimize every aspect of our lives including our genomes, faces, finance, emotion and environment have further added to the problem of privacy protection.The proliferation of AI technologies has impacted most of the spheres of our lives.

Many consumer goods and products which are using AI are equipped with sensors which generate and capture the data even without the knowledge or consent of the people. The data which is collected is then profiled to be used for marketing purpose and to make commercial gains and also to predict their future behavior. Anonymity of an individual is lost as AI methods are being used to identify people who wish to remain anonymous. Further, Artificial intelligence is also being used to infer and generate sensitive information about individuals from their non-sensitive data.

[40] https://www.thehindubusinessline.com/opinion/columns/slate/all-you-wanted-to-know-about/article24617362.ece

AI has become very attractive due to the speed, scale and automation. The speed at which AI does computations is already faster than what human analysts are capable of, and it can also be arbitrarily increased by adding more hardware.AI is also inherently adept at utilizing large data sets for analysis, and is arguably the *only* way to process big data in a reasonable amount of time. Finally, an AI can perform the designated tasks without supervision, which greatly improves analysis efficiency. These characteristics of AI enable it to affect privacy in a number of different ways:

a) Data Exploitation:

As the reliance on the AI technology is increasing so is the potential for exploitation. Many consumer products ranging from smart home appliances to computer applications are vulnerable to data exploitation by AI. With the use of AI, a person is unaware about how much data their software and devices generate, process, or share.

b) Identification and Tracking:

AI can be used for the purpose of identifying, tracking and monitoring individuals across multiple devices whether they are at work, or home or any public place. If the personal data is anonymised and once it becomes a part of a large data set, an AI can de-anonymize this data based on inference from other devices. This blurs the distinction between personal and non-personal data.

c) Voice and Facial Recognition:

Privacy and Anonymity of individuals is severely compromised with the use of two methods of identification that AI is increasingly adept at are Voice recognition and facial recognition. For example, Facial recognition and voice recognition are used by law enforcement agencies for the investigation purpose and to track the wrongdoers.

d) Prediction:

AI and sophisticated machine learning algorithms are being used to infer or predict sensitive information from non-sensitive forms of data. For instance, someone's keyboard typing patterns can be utilized to deduce their emotional states such as nervousness, confidence, sadness, and anxiety. Even more alarming, a person's political views, ethnic identity, sexual orientation, and even overall health can also be determined from data such as activity logs, location data, and similar metrics.

e) Profiling:

Data which is collected with the use of AI is profiled and can be used to sort, score, classify, evaluate, rank people. The data is collected usually without taking the consent of the data subject. Data subjects whose personal information is collected usually donot challenge the misuse as they do not have the ability and often helpless in tackling such issues.China's social scoring system is an example of how this information can be used to limit access to things like credit, housing, employment or social services.

Many governments have benefited by the Proliferation of Artificial Intelligence, enhanced IoT and IoLT devices. One such example is the use of Portable genome sequencer MinION and Metrichor which uses Artificial Intelligence in epidemiology which help to determine the risk of diseases. Sequenom Inc., is another example of the use of Artificial Intelligence which translates genetic code into relevant insights into genetic variations. On the basis of the data that is generated enables the government and other regulatory bodies to make informed decision to deal with and monitor the spread of diseases and to prevent epidemics. Tracking people can be done easily with Artificial Intelligence which in turn can be helpful to law enforcement agencies. Skydio's new biometric tracking drone helps law enforcement agencies to enhance their tracking capabilities. On the one hand, data capture and optimization potentially threaten our privacy and on the other hand both these processes are also vulnerable to cyber attacks conducted by governments and non state actors alike. This raises various concerns such as how are the companies and governments acquiring our personal data? Whether the citizens are aware of the data being generated on their daily interactions? In the face of comprehensive cognition and predictive intelligence how will the notion of privacy fare? The notion of privacy is undergoing change in the digital age and needs to be addressed. Many social media platforms like Google, Apple, Facebook, and Amazon (GAFA) comprise what some have called the tech oligopoly. Facebook for example had compromised the data of its users. Valuing Personal Data Framework was created by the World Economic Forum to outline the different elements of our digital avatars. Some of top most privacy concerns have been the lack of understanding of one's online presence; collection of data with implicit or reluctant consent; lack of control of one's personal data and privacy; deceptive use of terms and conditions agreements; and trading privacy for free services. The extent of digital mass surveillance has further raised questions regarding the extent to which international legal standards and national mechanisms sufficiently protect individuals from privacy breaches.[41]

VII. TACKLING THE PROBLEM -WAY FORWARD

Digital technologies like the AI have made our lives easier and have made substantial contributions in many areas of our lives. It is being used in many sectors like transport, health, education etc. The vast amount of data gathered can be analyzed with the use of the AI's and be used to solve many social ills. However, these technologies can also be misused by individuals, corporations, government and non-governmental agencies. Artificial Intelligence can also work to our detriment. One such example is the intrusion into privacy of an individual and misuse of data collected. To defend ourselves from exploitation by those who wield malicious intent is to manage and properly understand these technologies and their impact on our

[41] W Denton, Sarah & Pauwels, Eleonore & He, Yujia & G Johnson, Walter. (2018), *Nowhere to Hide: Artificial Intelligence and Privacy in the Fourth Industrial Revolution.*

lives. Further, it is high time for India to enact a comprehensive privacy and data protection legislation.

Sonia Katyal, the co-director of the Berkeley Centre for Law and Technology and member of the U.S. Commerce Department digital Economy Board of Advisors, has rightly predicted that, "In 2030, the greatest set of questions will involve how perceptions of AI and their application will influence the trajectory of civil rights in the future. Questions about privacy, speech, the right of assembly and technological construction of personhood will all re-emerge in this new AI context, throwing into question our deepest-held beliefs about equality and opportunity for all. Who will benefit and who will be disadvantaged in this new world depends on how broadly we analyze these questions today, for the future!"