IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA PROTECTION AND PRIVACY: NEED FOR RIGHTS BASED APPROACH AT THE AGE OF ARTIFICIAL INTELLIGENCE

SANDEEP T M

STUDENT

CHRIST UNIVERSITY DELHI

ABSTRACT

Privacy is recognised as the basic human right by most jurisdictions of the world including United Nations. Article 12 of Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights states recognise Privacy as inalienable basic Human Right. With the emergence of cutting edge technology of Artificial Intelligence, machine learning the threat of Data Protection and privacy has increased manifold. Dignity and individual liberty are under threat with the emergence of specialised algorithms under Artificial Intelligence which have the capacity to take parts of Data about a data subject from various inter-connected sources to generate sensitive personal data breaching the right to privacy of data subject. In this context any legislation about Data Protection should implement Rights based approach, instead of the consent based approach. The Rights based approach provides for certain inalienable Privacy rights to Data subjects and the corresponding duty on *the rem* especially the Data Collectors not to infringe on those rights which are provided to data subjects by the Data Protection Legislation. In case of any breach of rights conferred upon the Data Subject there would be a remedy against the breach. Right based approach shifts the onus on the Data collectors to not breach the rights of data subjects, the will be made liable to any breach of Data.

INTRODUCTION

In this digital era we are surrounded by variety of digital gadgets and these gadgets generate loads of data . One sort of data is that we may intentionally share, and the subsequent kind is the data which is produced in a real sense each time we accomplish something – regardless of whether it be travel, request a dinner or use transportation. There is no question that this data is enormously important and a few organizations are willing to pay for the access to this data. For sure, in this period of all-inclusive and essentially free access of web, data is the new cash. What is significantly fascinating is that the maximum utility of the data isn't known and cannot be imagined. As innovation advances, more up to date algorithms are developed to improve the worth of the data.

A few inquiries arise: who has the access to these data? where is this data stored ? who all have access to these data? Who are willing to purchase these data? How does this data help the purchasers in generating revenue for them? How can this data be abused? The ways to regulate these personal data and privacy? Is law able to catch up to the speed of development of newer intelligent technology? can the government get access to personal data of its citizens directly through them or through corporations having access to these data? Can the reason of security of state supersede the Rights of Privacy?

The discussion has now arrived at new levels. On August 24, 2017, the Supreme Court of India held that the 'right to privacy' is a major right ensured by Part III of the Constitution of India. This choice will have expansive consequences on the laws and guidelines. New laws will presently be tried on similar boundaries on which the laws that encroach upon individual freedom are tried under Article 21 of the Constitution of India. The right to privacy is presently unequivocally accessible – the inquiry that actually stays remarkable is its forms and cutoff points. That will be analyzed in another matter, for example the Aadhar case, which manages the obligatory biometric enrolment of everyone who's benefitting the government services in India.

As on date, India doesn't have an exhaustive enactment which manages data protection and privacy. The current enactments and approaches are basically sectoral in nature. Separately from other sectoral enactments, at this point, the applicable arrangements of Information Technology Act, 2000 and the standards there under, manage the collection process, and utilization of 'individual data', and 'sensitive individual data or data' by a 'body corporate' in India.

ARTIFICIAL INTELLIGENCE: MEANING, FUNCTIONS,FACETS

Artificial intelligence is a type of "intelligent computing" in which computer programmes can detect, reason, learn, act, and adapt in the same way that people can. It is "intelligent" in the sense that it mimics human cognition.

It is "artificial" because it includes the processing of computational data rather than biological data. The exponential development in computer processing and storage, as well as massive banks of data that can be probed to extract meaning, are driving AI's rising power. Many science fiction forecasts from the past appear to pale in comparison to the computational capacity of machines and improvements in robotics. The capabilities of AI will improve quicker than we can fathom or prepare for, with quantum computing on the horizon.

The large AI umbrella encompasses a wide range of systems. "Expert systems," for example, are sophisticated algorithms (stepwise computer programmes) that comprise a sequence of human-programmed rules and knowledge for issue solving. Machine learning (ML) is a more advanced kind of AI that relies less on human programming and more on an algorithm's capacity to learn from data as it proceeds. ML can be "supervised" (trained by humans) or "unsupervised," which means it is self-taught without human input. Larry Page and Sergey Brin, two Stanford University students, created an early implementation of the technology in 1997. They created a database of web ranks based on inbound link frequency. Google, the search engine they created, has grown to become one of the world's largest AI corporations. Deep Learning (DL) is a powerful form of machine learning that employs artificial neural networks, which are loosely inspired by the structure of the human brain. Artificial neurons are connected in layers that use "backpropagation" feedback loops to rewire and edit themselves on the fly. These are modelled after neuronal pathways in the brain, which strengthen with each use. DL uses this dynamic technique to detect patterns in unstructured data, which it then uses to model knowledge representation in a way that resembles reasoning. With DL, creators simply have to enter basic rules (such as mathematical operations) and goals, and the AI will figure out how to put them into action.[1] What makes AI so powerful is its ability to adapt.

The date when AI will be able to surpass human intelligence is hotly discussed. The Turing Test is a blind conversation experiment in which a human interrogator is unable to discern between human and computer-generated natural-language responses. Ray Kurzweil, a futurist, predicts that the Turing Test will be passed in 2029. Until then, we'll be stuck in an era of Artificial Narrow Intelligence (ANI), sometimes known as weak AI, in which special-purpose computer programmes surpass humans in tasks like skill games and text analysis. ANI encompasses cognitive computing, which involves machines assisting people in tasks like as assisting physicians in reading X-rays, stockbrokers in making trades, and lawyers in drafting contracts.

Artificial General Intelligence (AGI) will be the next generation of AI (AGI). Its powers will go beyond solving a pre-defined set of problems to incorporating intelligence into any situation. We will have achieved Artificial Super Intelligence when computers can autonomously exceed even the most intelligent humans (ASI). This has been dubbed the "singularity," when the capabilities of silicon computing surpass those of biological computation.[2] Visions of a gloomy future could emerge at that point. Fortunately, we have plenty of time to prepare. Unfortunately, we lack the necessary sense of urgency.

ARTIFICIAL INTELLIGENCE AND THREATS ON PRIVACY

Artificial intelligence is one of the cutting edge technology which has changed the face of Data science. Coupled with internet , its one of the most disruptive technology in the modern world. Varies applications of Artificial intelligence that surround us include self driving cars, Voice recognition systems , face recognition systems etc.,. Many applications of Artificial intelligence are not known to common man which deployed around us. Precision medical robots, Algorithms specially designed to analyse content

[1] *See* Alex Castrounis, *Artificial Intelligence, Deep Learning, and Neural Net-works Explained*, InnoArchiTech, https://www.innoarchitech.com/artificial-intelligence-deep-learning-neural-networks-explained ("[DL] algorithms them-selves 'learn' the optimal parameters to create the best performing model ... In other words, these algorithms *learn how to learn*.").

[2] *See* Ray Kurzweil, The Singularity is Near 136 (2005). John Von Neu-mann used this term to describe the point of technological progress "beyond which human affairs, as we know them, could not continue." Stanislaw Ulam, *Tribute to John Von Neumann*, 64 Bulletin Am. Mathematical Soc'y 1, 5 (1958).

etc.,. These applications and algorithms have the ability to process thousands of tera bytes of unstructured data with no or little economic value in to data which provide intelligible data of high economic value such as spending patterns and behaviours, political the ideology and others specific sensitive personal data. Artificial Intelligence has the ability to find solutions to various problems of world and it may bring in newer problems in the world of data privacy and Data Protection.

The fundamental right to privacy includes the freedom to make personal decisions for oneself , the right to keep one's personal information private, and the right to be left alone. These rights are widely recognised and protected in many post-World War II human rights charters, and they are considered basic democratic principles. The United States Constitution recognises the rights to decisional and informational privacy in an indirect manner, however this recognition is based on judicial inference rather than explicit mandate. As we will see momentarily, the constitutional and statutory protections for privacy rights in the United States encourage inventive and frequent invasions of those rights.

FORMS OF PRIVACY

Samuel Warren and Louis Brandeis' 1890 paper "The Right to Privacy," which explored and advanced the development of the common law "right of the individual to be left alone," is considered a fundamental work on information privacy. William Prosser crystallised four distinct harms arising from privacy violations as privacy rights evolved in the courts over time:

1) Intrusion upon seclusion or solitude, or into private affairs;

2) Public disclosure of embarrassing private facts;

3) False light publicity; and

4) Appropriation of name or likeness.

The four different injuries are now recognised as privacy-related torts in most states, with civil and criminal remedies available for the resulting causes of action. The privacy torts are intended to protect people whose feelings and sensibilities have been hurt by others discovering true, but intimate or embarrassing facts as a result of severely offensive behaviour.

Other concepts of privacy exist outside the common law origins of privacy and individuality. Informational privacy, decisional privacy, behavioural privacy, and physical privacy are all examples. The right to restrict the flow of our personal information is known as informational privacy. It applies to information we keep private as well as information we share in confidence with others. The right to make choices and decisions without being bothered or scrutinised is known as decisional privacy. The ability to do and act as one wishes , free from unwanted observation or intrusion, is referred to as behavioural privacy. The rights to solitude, seclusion, and protection from unlawful searches and seizures are all part of physical privacy.[3] As evidenced by their integration into foundational texts and a broad body of statutory, common, and evidential laws, these ideas of privacy have become a core aspect of Western democracy.

Informational privacy fosters a number of democratic ideals, including the freedom to generate ideas, experiment, think, and make mistakes without being seen or interrogated. Other freedoms are also protected, such as political involvement, religious freedom, economic freedom, and freedom from discrimination.

Information erasure these same liberties can be eroded by privacy. Others may be able to influence or control our actions if they have access to our personal information. That is why so many people want to get their hands on secret information. Our contacts; intimate relationships and activities; political choices and preferences; government records, genetic, biometric, and health data (pre-birth to post-death); education and employment records; phone, text, and email correspondence; social media likes, friends, and preferences; and government records, genetic, biometric, and health data (pre-birth to post-death). Data from our linked devices and wearable's, as well as browsing behaviour, location, and movement; purchase habits; banking, insurance, and other financial information; and data from our connected devices and wearable's. Every day, we generate a massive amount of data. It's a huge endeavour to keep it private. Penetrating our defences, on the other hand, can be very simple and profitable.

Data not only defines us, but it is also the lifeblood of artificial intelligence. Data science is the digital age's newest discipline. Companies like Face book, Snap Chat, and Google are essentially in the data business, not the social media or consumer tools business. The goods they give (which are usually free to the end user) are vehicles for collecting massive amounts of rich data, effectively turning the user into the product. Their business structures and revenue streams are driven by the precious commodity. Indeed, "personal data has become the most valuable commodity of the digital age, exchanged on a massive scale by some of Silicon Valley's most prominent firms and beyond."[4] As a result, society has become dataficated.

AI, with its ability to process massive volumes of data, jeopardises privacy in a variety of ways. In the parts that follow, we'll go over some of the ways AI can jeopardise our privacy and freedom of choice. Some of the methods presented were created prior to the development of AI. AI, on the other hand, may be used in all of them, making them more efficient and hence more dangerous. Indeed, we've already entered "privacy nihilism's" age.[5]

[3] Anita L. Allen-Castellitto, *Understanding Privacy: The Basics,* 865 PLI/PAT 23 (2006).

[4] Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.ny-times.com/2018/12/18/technology/facebook-privacy.html (describing how per-sonal data was traded among 150 companies without user consent).

[5] Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-pri-vacy-nihilism-is-here/568198.

USE OF DATA COLLECTION AND ANALYTICS

Due to the importance of data, technology corporations will continue to push legal and ethical boundaries in order to collect more data in order to construct models that make better and better predictions. The information is then shared with government authorities and private entities.

There are insufficient legal safeguards in place to prevent such disclosures. Understanding the complete picture, this shows that a large chunk of modern AI cannot exist without data, places data privacy and democracy at the top of the priority list.

Large-scale data acquired by IoT, surveillance, and tracking technologies is stored in various databases by data collectors or third-party "cloud" storage providers. Individual data sets dispersed across hundreds of servers may yield limited information insights when seen in isolation; however, this constraint can be overcome by a process known as "data fusion," which merges, organises, and connects those data points.[6] After the data has been collected, it is compared to a reference dataset. Deep Face outperforms the FBI's equivalent system in terms of accuracy.[7] Advances in AI's strength and speed have enabled such systems to identify an increasing number of potentially relevant insights from highly sophisticated and complicated data sets. Third parties create complex profiles of their "data subjects" using data that is collected, processed, and analysed, providing a wealth of usable intelligence to anyone looking to influence or manipulate purchasing decisions and other decisions.

The engine that drives data analytics is artificial intelligence (AI). It allows consumers to make predictions based on their financial, demographic, ethnic, racial, health, social, and other data. IBM's Watson, for example, offers Application Program Interfaces (APIs) that developers can use to design their own natural language interfaces. The Google Ten-sor Flow is an open-source platform and framework that allows AI developers to use machine learning to create a variety of applications. Facebook created "Deep Face," a deep learning facial recognition system that works by finding "principal components" in a photo and recognising them.

Advances in data collecting, analytics, and use pose a threat to privacy rights that aren't explicitly protected by state law's four privacy torts. Furthermore, they have the capacity to enrich as well as hurt society. Health data, for example, might be utilised for disease research as well as to reject candidates for lower insurance premiums. Everything from purchasing patterns to health status to religious, social, and political inclinations can be revealed through the aggregation and coordination of various records. The threat this poses has beginning to be recognised by the courts. Because of the detailed picture aggregated location information presents, a majority of the Supreme Court signed on to or concurred in support of a "mosaic theory," according to which long-term surveillance can be regarded a search in violation of the Fourth

[6] *See* Sadia Din et. al, *A Cluster-Based Data Fusion Technique to Analyze Big Data in Wireless Multi-Sensor Systems,* IEEE ACCESS (Nov. 2, 2021), https://ieeexplore.ieee.org/document/7873266 (describing data fusion).

[7] Russell Brandom, *Why Facebook is Beating the FBI at Facial Recognition*, VERGE (July 7, 2014), https://www.theverge.com/2014/7/7/5878069/why-face-book-is-beating-the-fbi-at-facial-recognition (97% accuracy for DeepFace vs. 85% for FBI systems).

Amendment. The government's capacity to store and mine this information for an indefinite period "chills associational and expressive freedoms", according to Justice Sotomayor's concurrence, and undermines the checks and balances employed to regulate law enforcement. If allowed, such unrestricted ability to track residents could have had a negative impact on government-citizen relations, posing a threat to democracy.

AI exacerbates and amplifies current patterns of data over-gathering and data use for unintended reasons not revealed to consumers at the time of acquisition. To train algorithms, supervised machine learning requires a significant amount of precisely labelled data. The larger the amount of data you have, the better your trained algorithm will be. The model becomes more sophisticated and potentially accurate as the number of variables or characteristics increases. As a result, the organisations that succeed will be those that have access to the best data, not the best algorithm. The algorithms will become smarter, faster, and more accurate as more data is collected. There is an incentive to collect and use a lot of data in order to build algorithms for new activities. The phrase "data is the new oil" was popularised recently to express the concept that data is a valuable commodity that can be commercialised.[8] Whoever has the most data, both in terms of quantity and quality, has the best chance of creating revolutionary business models and revenue generators.

INTERNET OF THINGS (IOTs)

The ability of a machine to access data is the source of artificial intelligence's power. AI essentially accomplishes the same thing: it crunches data. As a result, the more data points on a data subject or the larger the data set that can be accessed, the better AI will be at answering a query or performing a function.[9] The Internet of Things (IoT) is a network of electronic sensors that can be found on our bodies, in our homes, offices, cars, and public spaces. Any human-made or natural object having an internet address that sends data across a network without human-to-human or human-to-computer interaction is referred to as a "thing." If AI is analogous to the human brain, IoT is analogous to the human body collecting sensory data (sound, sight, and touch) (65). IoT devices get raw data from humans performing physical acts and interacting with others.66 Massive volumes of data have been collected, stored, and analysed thanks to these gadgets. 67Cisco anticipates that by 2020, there will be 50 billion new connected "things," one trillion by 2022, and 45 trillion in twenty years. Once those "things" capture our data, AI-based algorithms can use it to improve our lives while also influencing or controlling us. While the Internet of Things makes our every move and wish visible to data corporations, the gathering and use of our data remains a mystery to us. The massive information asymmetry leads to huge power asymmetries, with privacy being the primary victim.

[8] *The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (Nov 6, 2021), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
[9] *See generally* SAS, *Artificial Intelligence: What it is and Why it Matters,* SAS, https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelli-gence.html.

2. THE ECOSYSTEM OF SURVEILLENCE

We don't only come across "things" when it comes to data collection. They are accompanied by surveillance devices that are both real and virtual. Because of their widespread use, such systems appear to be innocuous or at the very least familiar. Consider Microsoft's Skype, Tencent's WeChat, or Facebook's WhatsApp and Messenger messaging apps. You use your data to pay for those free or low-cost services.[10] Consider email, text messaging, phone, cellphone, and IP voice telephony as well as other communication platforms. Your phone, as the old joke goes, now has three modes of communication: you, the person you phoned, and the government. When you add in communications providers that sniff your messages, collect your metadata, and follow your actions, you can see the breadth of the problem.

Aerial and satellite surveillance, drones, licence plate readers, street cameras, security cameras, infrared cameras, and other remote and augmented imaging systems are examples of visual methods that acquire personal data.[11]Google's "Sidewalk Labs" is working on a "smart city" that will use "ubiquitous sensing" to track all pedestrian and vehicular traffic. On the internet, there is no such thing as privacy. Here are a few of the causes for this. Small files called "cookies" are secretly placed on a user's hard disc to track his or her online movements and transfer that data to servers. The length of time spent on each page, activity, page scrolls, referring web site, device kind, and identity are all examples of user data acquired by "spotlight advertising," "web beacons," and "pixel tags." While users can set their browsers to "Do Not Track," there is no requirement that web sites honour DNT requests, hence the majority of them are ignored. Other privacy-enhancing solutions, such as virtual private networks, end-to-end encryption, and ad-blockers, are also available, but they are not always effective.

3. SURVEILLENCE BY THE GOVERNMENT

The federal government has mastered the technique of widespread surveillance, some of which is legal and some of which is not. Rather than surveying the numerous sorts of monitoring and Supreme Court decisions sustaining or rejecting them, we will focus on the forms and theories that contribute to AI's loss of privacy rights. The third-party theory states that when the government acquires data about a subject indirectly via a "third-party" rather than directly from the subject, the Fourth Amendment does not apply.[12] The traditional jailhouse informant, who has gained information from a suspect and can freely offer that information to the prosecutor despite the defendant's opposition, is a famous example. However, the doctrine goes far beyond. Anyone who divulges otherwise protected information to a third party may have "misplaced faith" in that person and thereby forfeits whatever expectation of privacy she may have had previously. Because of the misplaced trust and third-party doctrines, the government can get information

[10] *See* Samuel Gibbs *How Much Are You Worth to Facebook,* GUARDIAN (Nov. 2, 2021), https://www.theguardian.com/technology/2016/jan/28/how-much-are-you-worth-to-facebook.

[11] Robert Draper, *They Are Watching You – and Everything Else on the Planet*, NAT'L GEOGRAPHIC (Dec. 2017), https://www.nationalgeographic.com/maga-zine/2018/02/surveillance-watching-you.

[12] Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third par-ties").

about you from anyone who has it without violating any statutes or common-law prohibitions. Travel firms and GPS-enabled programmes (such as Waze and Google Maps), which gather travel history and searches, to financial service entities (such as Medical care providers and insurance, who have patient medical records, to banks and credit businesses, which have clients' financial information.

There isn't much information that a third party doesn't already have or has access to. The Health Insurance Portability and Accountability Act (HIPAA),[13]the Electronic Communications Privacy Act (ECPA),and the Fair Credit Reporting Act all provide federal legal protections (FCRA).However, these only cover a small portion of the total number of entities. Most others have a privacy obligation based on a contract (Terms of Use agreements), state law, or a common-law fiduciary relationship. The majority of those provisions allow exceptions for requests for records from law enforcement or the courts.

4. CONFIDENTIALITY

While informational privacy is concerned with keeping our activities hidden from others, anonymity allows us to reveal our activities while being anonymous. It allows involvement in the public arena that would otherwise be impossible if associations were made public. "Anonymity is a protection from the tyranny of the majority," the Supreme Court observed in McIntyre v. Ohio Elections Commission. It so exemplifies the goal of the Bill of Rights, and specifically the First Amendment: to shield unpopular people from retaliation at the hands of an intolerant society."[14]

A famous New Yorker cartoon depicts a dog surfing the web and telling another dog, "On the Internet, nobody knows." "You're a canine." That may have been true before AI, when comparing IP addresses to other data was time-consuming. However, things are no longer so straightforward. Anonymisation is the process of removing personally identifiable information from acquired data, making it impossible to identify the original source. Pseudonymization, a related technique, substitutes most identifying data elements with pseudonyms or fictitious identifiers.[15] It includes techniques such as hashing, data masking, and encryption, all of which minimise the likability of datasets containing personal information. The existing legal distinction is that data that has been pseudonymzed can be re-identified (e.g., reconnecting the individual to their information). The law, on the other hand, ignores AI's potential to re-identify anonymised data. By extracting relationships from seemingly unrelated data, AI is brilliant at re-identifying (or de-identifying) data. Through their apparently anonymous medical billing records, a University of Melbourne study was able to re-identify certain Australian patients. With credit card metadata, you can get similar results.

[13] 42 U.S.C. 201. Most HIPAA requirements were promulgated by regulation by the Department of Health and Human Services. See 45 CFR 160.100, et seq.

[14] 514 U.S. 334, 357 (1995).

[15] Clyde Williamson, *Pseudonymization vs. Anonymization and How They Help With GDPR*, PROTEGRITY (Nov. 5, 2021), https://www.protegrity.com/pseudony-mization-vs-anonymization-help-gdpr.

C. PRIVACY DECISIONS (AUTONOMY)

Autonomy is derived from the Greek words autos (self) and nomos (rule) (rule). The Greeks used the phrase to denote political autonomy.[16] However, its importance to democracy has expanded to include other kinds of autonomy, such as the right to make decisions about oneself and one's life paths, which we refer to as "decisional privacy."[17] Self-governance, liberty rights, privacy, individual choice, liberty to follow one's will, causing one's own behaviour, and being one's own person are all terms used today to describe autonomy. Autonomy is closely linked to free will and is necessary for human dignity and individuality.

ARTIFICIAL INTELLIGENCE ANF THREAT TO SOCIAL VALUES AND DEMOCRACY

Advances in Artificial intelligence presage not only a new era in computing, but also new threats to societal ideals and constitutional rights. The dangers of social media algorithms and the Internet of Things to privacy are well-known. The even bigger threat that AI poses is to democracy itself which is underappreciated and uncalled for[18]. Recent instances demonstrate how artificial intelligence (AI) can be "weaponized" to rig elections and undermine public trust in democratic institutions. The law, unlike many other disruptive technology, is slow to catch up. Indeed, more than a half-century after the military and scientific organisations began serious research, the first ever congressional hearing on AI was held in late 2016.

Many centuries-old societal conventions and structures have been upended by the digital age. Core principles such as personal privacy, autonomy, and democracy are among the most important. These are the origins of liberal democracy, whose power in the late twentieth century was unprecedented in human history. At the turn of the century, technological advancements promised a bright future in human well-being. But then the warning flags started to surface. The internet gave birth to social media, which has had a dramatic and seemingly irreversible impact on privacy. Many functions have been beneficially automated as a result of the Internet of Things (IoT), which has resulted in ubiquitous monitoring and control over our daily life. The rise of "Big Data" and data analytics is one result of the internet and IoT. Consumers, viewers, and voters can be influenced in complex and covert ways using these techniques. The loss of autonomy in personal decision-making that has resulted has been just as significant as the loss of privacy.

[16] *Autonomy*, MERRIAM-WEBSTER DICTIONARY ONLINE, https://www.merriam-webster.com/dictionary/autonomy (last visited April 22, 2019).

[17] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (finding "a right to privacy in the 'penumbras' and 'emanations' of other constitutional protec-tions.").

[18] *See* Nicholas Wright, *How Artificial Intelligence Will Reshape the Global Order*, FOREIGN AFF. (July 10, 2018), https://www.foreignaffairs.com/arti-cles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

The erosion of trust in and control over our democratic institutions is perhaps the most significant societal cost of the new technological era of AI[19]. Cambridge Analytica's "psychographic profiling" of Face book users during the 2016 elections in the United Kingdom and the United States are two examples. However, voting manipulation is far from the only danger that AI brings to democracy. The scope of constitutional rights is shrinking as more and more government operations are privatised. Relegating these functions to artificial intelligence allows for secret decision-making that is not subject to public inspection or supervision. Predictive policing and AI sentencing in criminal cases, for example, might encourage prejudiced societal behaviours while pretending to be objective. Similar algorithmic biases can be seen in various areas of decision-making, such as credit, employment, and insurance. "Machines are already being given the ability to make life-altering judgments regarding people on a daily basis." They do so without responsibility or transparency.

Advanced manipulation technologies have advanced to the point that people believe their judgments are their own, although they are often "directed" by algorithms . "Big nudging," a type of "persuasive computing" that "allows one to efficiently rule the masses without having to involve citizens in democratic processes," is a good example[20](5).Political participation is discouraged. One of the goals of people who utilise AI to manipulate and control humanity .

Threats to privacy and democracy undermine human values both collectively and individually. Unfortunately, at least in the United States, industry self-regulation has been mostly responsible for monitoring these existential trends. Little has been done at the national level to maintain our democratic institutions and principles. There is minimal regulation of AI research, allowing digital behemoths to freely browse our data and infringe on our rights. We appear to be in a scenario where Facebook and Google CEOs Mark Zuckerberg and Sundar Pichai wield more power over Americans' lives and futures than the lawmakers we elect. The potential of AI software ("West Coast Code") to undermine or displace regulatory law ("East Coast Code") gives these tech behemoths the power to behave as "Emergent Transnational Sovereigns". The developing AI landscape has been dubbed "digital authoritarianism" or "algocracy"—rule by algorithm.

This article examines the current and future threats that artificial intelligence poses to basic democratic concepts such as privacy, autonomy, equality, the democratic process, and the rule of law. Some of these threats predate AI, such as clandestine manipulation of consumer and voter preferences, but they are made even more effective by AI's massive processing power. The unique dangers of AI, on the other hand, are more concerning. For example, AI's capacity to construct detailed behavioural profiles from varied datasets and re-identify anonymised data is one of these capabilities. Advertisers, governments, and strangers have access to our most sensitive information. Social media companies, who rely on AI to fuel their development and revenue models, are the biggest dangers here. "Algorithmic bias" and "unexplained AI"

[19] *See, e.g.*, Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 195 (2017) (the AI-enabled "ecosystems constructed by Google and Facebook have contributed importantly to the contemporary climate of political polarization and distrust"); *infra* Section IV.A.4.

[20] Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 25, 2017), https://www.scientificamerican.com/arti-cle/will-democracy-survive-big-data-and-artificial-intelligence .

are two more innovative qualities that have sparked debate. The former refers to AI's proclivity to reinforce societal prejudices invisibly and under the guise of impartiality. The lack of transparency in AI is described by the latter. The findings of AI are frequently dependent on reasoning and processing that people are unaware of. In that they prevent AI outputs from being checked against constitutional principles, the opacity of AI "black box" decision-making14 is the opposite of democratic self-governance and due process.

We do not underestimate AI's productive benefits or its unavoidable direction, but we believe it is also vital to emphasise its perils. This isn't a vision of a gloomy future, as many grim predictions about AI have suggested.

At its most basic level, AI mimics human information sensing, processing, and response—what we may loosely refer to as "intelligence"—but at far faster rates and scale, generating results that humans could never achieve. IoT and Big Data Analytics are examples of AI data collection and processing features. To work properly, AI requires a lot of data, which means a lot of personal data. AI will most likely erode human rights to decisional and informational privacy as a result of this process.

NEED FOR RIGHTS BASED APPROACH AT THE AGE OF ARTIFICIAL INTELLIGENCE

The rights-based model (Rights Model) will aid in safeguarding the interests of data subjects who share their information with data controllers. Every individual has an unalienable right to his or her personal data under this Rights Model. Any data collector who intends to gain access to a data subject's personal data must do so in a way that does not infringe on this inherent data right. As a replacement for the Consent Paradigm, this Discussion Document lays out the features of a rights-based model (Rights Model). The following are the characteristics of the Rights Model:

- It ensures that everyone has access to a set of data rights,
- It shifts the duty of assessing the privacy risk to personal data from the data subject to the data controller, compelling the data controller to be aware of its data collecting, processing, transfer, and storage activities. When the state acquires / processes personal data, the Model applies equally.
- It focuses on the harm caused to the data subject as a result of a violation of his data rights, and it provides him with a remedy regardless of whether he has agreed to the provisions of a privacy policy. Once a harm to the data subject has been established, the accountable data controller will be held liable.

THE CONSENT MODEL'S SHORTCOMINGS

There are three major reasons that the Consent Model is no longer viable:

1. **The Consent Model is insufficient, resulting in "consent fatigue."**

Because there were few reasons to acquire data and few further uses to which it might be put previously, the Consent Model sufficed. Data was static once it was acquired, and it was rarely shared outside of the company. As a result, data subjects had a clear understanding of what data was being gathered and for what purposes it would be used, allowing them to make informed decisions. The Consent Model was both possible and adequate in this situation.

This isn't the case anymore. There are far too many ways to collect, analyse, transfer, and consume data nowadays to list them all. Recruiters can examine our employment histories as well as our social media activities because our online activity is tracked and our buying choices are documented. Every financial transaction we make is tracked and associated with our location, age, and time of day, providing unseen insights about our personalities. Smart devices with sensors and cloud intelligence surround us, tracking our activities and logging what we do and how we do it. We sign standard form contracts that are dense and convoluted, making it difficult to analyse the ramifications of consenting to the provisions set forth therein. Consent fatigue develops as a result of this, as well as the sheer amount of contracts we end up signing. This leads to decreased consent, in which we agree to the terms of service and give our assent without reading the fine print. According to a research released in 2008, if everyone took the time to read privacy policies thoroughly, the national opportunity cost of that time in the United States would have exceeded $781 billion at the time.

2. **The rise of interconnected databases increases the need to protect individual data**

Modern databases are built to be interoperable, with APIs allowing them to connect to other datasets. Data controllers can overlay numerous sources of data and provide valuable insights about data subjects because to this interconnectedness. Consent to such exchanges of personal data is now commonly included in privacy rules.

As previously stated, evaluating the impact of a privacy policy in the context of indirect data collecting is extremely challenging. It's nearly impossible to assess the impact of interconnected datasets, especially when the insights revealed are typically unforeseen.

3. **The rapid increase in data transformation threatens personal privacy**

When collecting non-personal data in India, there is no legal necessity to get prior consent. Machine learning algorithms are now capable of connecting seemingly unrelated data chunks, detecting trends, and constructing accurate personal profiles. As a result, divergent data elements are effectively converted into sensitive personal information. In these scenarios, permission would be insufficient to protect us from the potential harm that deep learning algorithms can cause.[21]It's worth noting that machine learning algorithms and neural networks are built to run without the need for human intervention.7. As a result, even the most experienced data scientists will be unable to predict how these algorithms would interpret the data they are given.

THE RIGHTS MODEL'S FOUNDATIONAL PRINCIPLES

The Rights Model should be based on the concepts of accountability, autonomy, and security to ensure that data subjects are not denied access to their data and that data controllers are held accountable for any privacy violations.

Any viable alternative to the Consent Model must address the following difficulties. It must ensure that data controllers who have access to data subjects' personal information are held accountable for any harm they cause, regardless of whether the data subject has given their consent. Because privacy is a personal boundary, the model must also ensure that each individual has the liberty to define his or her own privacy limits, as well as the power to limit the purposes to which data controllers can put his or her data.

In light of this, the suggested Rights Model should be governed by the following fundamental principles:

1. Accountability

Data controllers must be accountable for the information they have in their possession. If a data subject suffers harm as a result of a security breach or the data controller's processing of the data, the latter must be held liable. This liability must exist regardless of the data subject's consent.

The Accountability Principle's Importance

In comparison to the Consent Model, the accountability principle assigns a higher level of duty to a data controller. It does so by addressing the flaws connected with ideas that are frequently mentioned in other countries' privacy acts. These principles, which are frequently extensions of the concept of consent, include the following:

The concept of choice, which states that a data subject should be able to choose whether or not his personal data should be collected and processed. This assumes that data subjects are aware of the consequences of permitting their information to be collected and processed.

[21] Learning Hannah Devlin, Discrimination by Algorithm: Scientists Devise Test to Detect AI Bias, The Guardian, 19 December 2016 (last visited Nov 2 2021).

The ideas of purpose limitation and use limitation, i.e., data collectors must ensure that data is acquired for a defined purpose and then processed only to the degree necessary to fulfil that purpose. Limiting use and purpose in relation to what the data subject has consented to is meaningless because obtaining meaningful informed permission is nearly impossible.

A prohibition on the unintentional disclosure of personal data to other people or organisations. This restriction stems from the idea that the best method to preserve personal privacy is to prohibit data dissemination unless the data subject has given their consent. This idea presupposes that data subjects are capable of evaluating information whether or not a specific disclosure or transfer may compromise their personal privacy.

2. Autonomy

All data subjects should have control over their information. Because it is impossible to successfully prevent data gathering in the age of current technology, every data subject should have the opportunity to limit or restrict how data is handled once it has been obtained.

3. Safety and security

From the moment data is collected to the moment it is processed and used, it must be handled with care. Even if no harm results from the loss of data as a result of a security breach, the data controller must be fined or imprisoned as appropriate for non-compliance.

CONSEQUENCES OF THE RIGHTS MODEL

After outlining the general principles upon which the new data protection law should be founded, we will now go over the specifics of the proposed legislation.

1. **Every person has some unalienable rights to their personal information.**

A set of data rights will be granted to data subjects. When dealing with a subject's data, a data controller will be required to guarantee that these rights are respected. While there will be no restrictions on the collection or processing of data relevant to a data subject, and hence no requirement to get that person's agreement prior to collection, the new framework will be predicated on holding the data collector responsible for any harm caused. As a result, the data collector will have a fiduciary responsibility for the data under its control and will be accountable for any harm made to the data subject as a result of that data.

We recommend that personal privacy be safeguarded by enacting legislation that provides all people with a set of data rights. These rights, which apply to both personal and non-personal data, can be used by data subjects to take action against anybody who processes or possesses their data. Unlike the previous framework, which limited data subjects' rights to those with whom they had contractual ties, the new framework guarantees that data subjects' rights to their data are inalienable and unaffected by any restrictions and conditions. Data controllers will be unable to claim consent as a defence to avoid liability because the right is available in rem (i.e., against the entire world). In fact, data controllers will be required to ensure that the data subject's rights are not breached as a result of the way the data was acquired or processed.

The data rights shall include the following:

a. The Right to Fair Treatment:

When a data controller arrives at a judgement or makes a judgement about the data subject by processing any data, the data subject has the right to be treated without bias. Because machine learning is primarily reliant on patterns to generate decisions, bias is easy to introduce8. As a result, patterns emerge that are stable but occasionally discriminatory.

For example, a bank's machine learning system finds a pattern and utilises it to decide that loans should not be issued to persons from backward castes based on the data already supplied into it. On the basis of this conclusion, a data subject from a backward caste with good credit is unjustly denied a loan. The proposed statute will allow offended data subjects to allege that they were harmed as a result of biassed data processing because it clearly provides for the right to fair treatment.

b. **The Freedom of Information Act (FOIA):**

The data subject has the right to access information about all personal data about him held by or controlled by a data controller. The data subject must have the right to know what use his or her data has been put to, as well as the people or entities with whom his or her data has been shared and who has had access to it. The data subject shall also have the right to have any inaccuracies or omissions in the data that are within the data controller's power to be corrected, provided that the errors or omissions are verifiably true.

C. The Right to Data Protection:

The data subject has the right to be guaranteed that his data is secure at all times. This means that data controllers must store all data under their control in a secure manner. Furthermore, such data must be processed and transferred in accordance with appropriate security policies and procedures.

d. **The Right Not to Be Processed:**

Data subjects who do not want their data processed have the right to demand that the data controller immediately stop processing their data. Rather than presenting only binary options, the statute could be applied in such a way that the data subject has granular control.

The data controller, for example, could be required by the statute to display the data subject all of the ways his data is handled. The data subject might then granularly withdraw consent to the processing of specified categories of data via an interactive dashboard. The interactive dashboard should be designed to notify the data subject about the implications of withdrawing consent on the services offered (for example, withdrawing consents to collect location data).

CONCLUSION

Artificial intelligence pose the problem of surveillance ecosystem, surveillance by the government, breach of confidentiality, threat to autonomy, specially threat to social values and democracy and many other ill-effects on privacy issues.

With these issues and threats arising out of Artificial Intelligence, it is imperative to adopt Right based legislative model than consent based model. The Rights based model shifts the duty of assessing the privacy risk to personal data from the data subject to the data controller, compelling the data controller to be aware of its data collecting, processing, transfer and storage activities. When the state acquires, processes personal data , the model applies equally.