IOSR Journal of Humanities And Social Science (IOSR-JHSS)
Volume 26, Issue 4, Series 3 (April. 2021) 39-48
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Socio-legal Impact on Privacy in AI-Driven World

[*]Mayank Tiwari
[**]Atul Kumar Pandey

Date of Submission: 25-03-2021 Date of Acceptance: 09-04-2021

I. INTRODUCTION

Privacy has been the word for the information age, especially with exponential growth in internet-based activities. Privacy has no one definition, and *Rick Falkvinge* has defined it in various forms, segregating it into seven categories[*].

- Privacy of Body - This implies that a person has the fundamental human right over their own body. No other person or government institution can examine or invade into it through blood tests, fingerprint scans, narco-analysis etc.
- Privacy of Correspondence - This means that all communications, whether carried verbally or over digital space, remain private between the persons having it. The recent discussions and debates over WhatsApp privacy policy and increased usage of Signal messaging application convey that the public is now more aware of their conversational privacy.
- Privacy of Data - This means the data generated by every person over any platform, like social media, government bodies, personal devices like mobile phones or laptops etc. Being a diligent digital citizen and using security mechanisms like antimalware and encryptions tools help secure data privacy.
- Privacy of Finance - This is a new approach towards privacy and is upcoming with the advent of bitcoins and digital currency. The cut down the tracking of money through public and private banks, people have started investing in bitcoins, where all transactions are secured and privatised in a ledger structure using blockchain technology.
- Privacy of Identity - This means the right to remain anonymous. As much as the government needs to implement security measures like street cameras for the functioning of law and justice, they have also become a tool of mass surveillance, leaving the public with no other resort. Robust access control mechanisms, identity cards and effective laws and judicial operations are a few ways to protect identity privacy.
- Privacy of Location - This means that persons have the right to be wherever they want without government bodies tracking their movements. However, the installation of GPS devices, social media posts have brought this privacy aspect under grave concern.
- Privacy of Territory - This kind of privacy discusses a person's right to their belongings, not only pertaining to their houses but cars, place of business etc. No other person or government body should be allowed to invade unannounced and take charge.

Therefore, from understanding the above different kinds of privacies, privacy can be defined as a person having the right to keep their information to their own or a limited few, with consent. Privacy has been considered an exercise of human rights since the beginning of time, protecting dignity, the freedom to express or associate. Privacy is also regarded as cultural in nature, what a citizen from one nation may share easily with a stranger, another nation's citizen might not find appropriate to do so.

In the information age, with the advent of big data, automation and artificial intelligence, it becomes all the more difficult for a person to protect their data, as it becomes easy for big corporations to collect, modify, store, retain and exchange data within and outside their organisational structures. Privacy has therefore become both a social and a legal issue in this new age. The emergence of artificial intelligence only accelerates the governmental and corporate bodies to regularise techniques that affect people's privacy without their consent.

[*] Assistant Professor, National Law Institute University, Bhopal.
[**] Associate Professor, National Law Institute University, Bhopal.
[*] Rick Falkvinge, *Our Seven Privacies: The Many Important Facets of Privacy*, (Privacy News Online, 13 Nov 2013), https://www.privateinternetaccess.com/blog/our-seven-privacies-the-many-important-facets-of-privacy/#:~:text=There%20are%20seven%20distinct%20important,invade%20it%20without%20your%20consent. Accessed 4 Feb 2021.

The domain of artificial intelligence brings new factors to affect privacy by the capability of collecting large amounts of data, spread across global servers, for a worldwide audience and the ability to process it at high speeds and seek results that are more accurate than human-generated results. The technology to analyse data and learn from past data without supervision is only the beginning of the power of artificial intelligence. The possibilities of artificial intelligence are vast, and thus it is often seen as an emerging evil. The public needs to be made more aware of it, its functioning and its powers to tackle it.

Following are a few ways how artificial intelligence can affect privacy[†]:

- Data Exploitation - Many applications come preinstalled in user devices with default permissions to their activities, such as access to audio-video files, messages, camera, location. The AI running at the backend periodically sends this data across servers that get stored and primarily used for unsolicited marketing via mails, messages and within app advertisements.
- Identification & Tracking - AI is heavily used for collecting data over multiple devices and analysing their result. This leads to smart devices giving out information that a user may not even be aware of, as their preferences on movies, food, clothing and locations, and lead to creating a database, which is then used to identify and track their activities.
- Voice & Facial Recognition - These technological advances of AI highly compromise every individual's privacy. These are deployed majorly in every city for implementation of the law to get hold of law-breakers. Social media and smart devices have further aggravated the situation by using this biometric information to create the database on individuals without explicit consent.
- Prediction - The data collected over a period of time, even against one person, can tell a lot about their personality, such as google searches might lead to private information such as health information or location, typing patterns may disclose psychological traits and nature of the use of websites may speak about their political opinions or sexual orientation.
- Profiling - From the kind of information collected over time of individuals, it is easily possible to create a database of all such activities, which is updated and enhances with subsequent data. When this database studies and analysed to target individuals for governmental, private or corporate reasons, it is called profiling. The individual in such cases has very little recourse to regain their data or have it removed from different servers. However, laws have lately become proactive towards this.

The challenge remains to be precautious of misuse of data than to seek compensation post its misuse. This paper, therefore, discusses the impact of artificial intelligence in the social and legal aspect. It also studies artificial intelligence in layman terms and looks forward to a way out of the uncertainties that artificial intelligence has to seem to create.

II. ARTIFICIAL INTELLIGENCE FOR LAYMAN

Artificial Intelligence is a field of computer science that aims to create computer programs that can imitate humans in terms of the tasks they perform. A program is taught in the same manner that a human child is taught, that is, through repeated actions, adapting, pattern recognition and reinforcement learning. Since the nature of information taught is computerised and fed into the program by inputting large amounts of data, it's called artificial. Since the tasks performed or sought to achieve is that of a human creature, it's called artificial intelligence. The origin of AI remains disputed, however, the development of the Turing test in 1950 gave the concept of AI a new direction and made everyone realise that it's here to stay. The past 20 years have seen tremendous study, progress and sky-rocketing results from the innovations in AI algorithms. The vastness of its application in every possible existing field and the ability to create new fields is mind-boggling. The foundational thought that whether a machine can think has brought humans to experiment with this piece of technology to question the very basis of thinking, processing data, and creating a life-like supporting program that exhibits this nature. Artificial intelligence, however, remains an overarching umbrella term for all its various kinds. The same are discussed below to give a ground perspective on the extensiveness of the application and execution of AI programs.[‡]

a. Narrow, General and Super Artificial Intelligence

Narrow AI refers to those AI systems that are programmed to perform and act upon a singular or specific task. For instance, Deep Blue by IBM was trained and tested to play Chess and even won against the world's chess champion. However, Deep Blue cannot be expected to do a task as simple as putting a plate on a dining table. Therefore narrow AI is designed for specific tasks and only perform what is intended. Currently, all innovations in AI fall into this criterion. General AI refers to the intelligence of a human being. To simplify

[†] Michael Deans, Towards Data Science, *AI and the Future of Privacy,* (Towards Data Science, 5 Sep 2018), https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4 accessed 4 Feb 2021.

[‡] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies,* (1st Ed, Oxford University Press, 2014)

this, consider a human watching a monkey climb a tree and a fish swimming. Now the monkey cannot swim, and neither can the swim climb the tree, but the human watching both can apply its intelligence and learn to do both. Therefore, to sum general AI, it is to be able to match the intelligence of a human. Superintelligence, lastly, refers to a stage when AI would advance so considerably that it will outsmart the combined intelligence of the world's smartest minds. This stage may seem far, however, given the exponential growth of AI, experts in the field expect it to be emerging within the next 30 years and thus creating the debating of human versus machines and settling a fear in society that machines will become too powerful to control and lead to termination of human existence.

b. Big Data

Big Data and AI go hand in hand. AI systems function on the requirement of being fed large sets of data, and big data refers to the humongous amount of data collected at all times, across all devices. It is the vastness of the data that gives it this name. Users knowingly and unknowingly create a large amount of data throughout their day-to-day activities like the places they visit, search histories, social media posts and reactions. All this data is collected, analysed, processed, stored etc. and forms part of the big data. The complexity factor comes in when no traditional data management methods can control or even store this data, which might lead to leakage of data and present a huge breach of user privacy.

c. Machine Learning & Deep Learning

Machine learning is a subset of Artificial intelligence, and deep learning is a further subset of machine learning. They both are heavily dependent on mathematics, probability and statistics. Machine learning refers to the program learning from its past outcomes and results. Deep learning solves complex machine learning problems that involve more than information, such as media files like audios and videos. Both require a large quantity of data to train and test upon for more accurate results and reduce false positives. They both differentiate on the kind of data that is fed into the models. Machine learning builds on labelled data, whereas deep learning builds on unlabelled and unstructured data. This feature also makes machine learning models more transparent, and deep learning models be more opaque in their explainability towards algorithmic logic. Though deep learning models take a longer time to train and test, they are more accurate in results than machine learning models. Together, they both form the core of any artificial intelligent system that helps in providing results that more accurate than human-generated results and that too at high speeds. The efficiency aspect of AI is unbeatable in front of humans, raising the concern of humans getting replaced at many job profiles in coming years.[§]

d. Natural Language Processing

Natural Language Processing, or NLP, is the branch of artificial intelligence that improves the interaction between humans and machines. This is done by way of recognising both audible and textual speech and understanding the semantical and syntactical analysis of it to interpret the data and provide a meaningful response. Few application of NLP in daily life are Echo, Siri, Google voice assistant. Many websites, private and government, also offer an NLP AI assistant in the form of a chatbot that responds to specifically trained queries. Customer relations management, digital marketing and chatbots in various fields have transformed exponentially because of extensive study of this branch of AI.

III. SOCIAL IMPACT

Society and privacy go hand in hand, and one is bound to affect the other. The incoming of AI has impacted both in a grave manner, affecting lives globally. Following are few instances of how AI has socially impacted privacy:

1. The Cambridge Analytica-Facebook Scandal

In 2010, Facebook changed its policies to allow external developers to access users' personal data and their friends using Open Graph. This feature was used by a company named Global Science Research in 2013, run by Alexander Kogan, using an application called 'this is your digital life', developed to create psychological profiles of users on FB. It involved Data Analytics via Machine Learning Algorithms that were fed training data sets from paid surveys and online quizzes and predicted a more accurate pattern than human-formed data; all made possible with the help of emerging domains of cyberspace. The analysis categorised people on a scale of five essential features of human personality and psychology, namely, conscientiousness, extraversion,

[§] Information Commissioner's Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (ICO UK, Sep 2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf accessed 5 Feb 2021.

agreeableness and neuroticism. It involved the use of microtargeting and voter profiling, sending out disinformation through memes, posts, trolls, false statistics etc., in accordance with the behaviour of the persuadable to influence their thoughts. There also existed cross-border transfer of data and information, that is, US to UK and Russia, nations that have not been allies since centuries. Two years later, the Guardian reported a State senator was using this data for election campaigns, and soon after, Donald Trump started heavily investing in FB ads. In 2018, a whistle-blower from now named Cambridge Analytica exposed the profiling of over 80 million Facebook users, and investigations began into violation of Facebook's policies. The company was fined an amount of whopping 5 billion and reassessment of privacy policies.[**]

2. Clearview Face Recognition Scandal

Clearview is a company that heavily uses artificial intelligence and machine learning algorithms to create software to recognise faces over a large number of data. Their objective started to assist the executive pillar of government in tracking law-breakers, terrorists, traffickers, etc. However, the biggest shock came to the world when only last year, the renowned New York Times published a detailed report on how Clearview has been escaping their privacy policies and exploiting data from users worldwide, without their consent illegitimately. It was found out that the company had used over 3 billion photos available over Facebook, Instagram, Twitter, YouTube, Venmo and other social media handles to feed as training data and into their machine learning algorithms. All the social media organisations sent a cease and desist letter to the company, who claimed that these photos were publicly available. This kind of gross privacy violation reeks of the flaw in the functioning of artificial intelligence methods because this can easily lead to identification and persecution of innocent citizens as the algorithm may result in false negatives or gets into the hands of wretched police officers.[††]

3. DeepFakes

Deepfakes are modified audios, image files or video content created using a branch of artificial intelligence. Deepfakes are declared to be the most notable development in the field of artificial intelligence and have been seen to bring the potential of extreme use in various industries. Deepfakes have plenty of positive uses in numerous industries, ranging from entertainment to healthcare. However, they are instead infamous for their nature of work and state of the art. A recent survey revealed that approximately 96% of all deepfake content on the internet is pornographic. Since there is a huge amount of publicly available data on celebrities regarding their images and videos, it becomes a resourceful place for training the algorithm from such a vast dataset. In 2017, the first deepfake emerged with a face of a celebrity swapped over that of a porn actor. It is also of grave threatening concern that a significant percentage of these pornographic deepfakes is revenge porn. A more grave instance was recorded in 2019, wherein an application called DeepNude allowed the swapping of the face of any women over nude images and videos. The application was soon shut down after the controversy on its nature, but it gives an insight into the misuses of this technology.[‡‡]

4. Mass Surveillance

AI surveillance technology is spreading faster to a wide range of countered than experts have commonly understood. From the Snowden leaks in mid-2013 to the interest surrounding a US court's ruling that Apple decrypts a terrorist's iPhone, the words' mass surveillance' is commonly used to describe many sorts of privacy infringement. Mass surveillance is the practice of spying on a whole or significant part of a population. It can involve anything from CCTV monitoring and email interceptions to wire-tapping and computer hacking. Often, mass surveillance is administered by the state, but it also can be administered by corporations, either on behalf of the state or on their initiative. Despite its advantages, face recognition technology also poses a significant number of risks. It enables and normalises blanket surveillance of people across numerous environments. This makes it the right tool for oppressive governments and manipulative corporations. In recent years, China has received severe criticism because of the mass surveillance of its people without their consent.

[**] Elena Boldyreva, *Cambridge Analytica: Ethics and Online Manipulation With Decision-Making Process,* (St. Petersberg Polytechnic University, Dec 2018), https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process accessed Feb 4 2021.

[††] Nick Statt, *Clearview AI to stop selling controversial facial recognition app to private companies,* (The Verge, 7 May 2020), https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law accessed 4 Feb 2021.

[‡‡] Jacob Kastrenakes, *Controversial deepfake app DeepNude shuts down hours after being exposed,* (The Verge, 27 June 2019), https://www.theverge.com/2019/6/27/18761496/deepnude-shuts-down-deepfake-nude-ai-app-women accessed 4 Feb 2021.

They use over 200 million surveillance cameras and biometric identification to keep a relentless watch on their people. China also mines their behavioural data captured on the cameras. To make it worse, China implemented a social system to rate the trustworthiness of its citizens and provides them ratings accordingly supported their surveillance. People with high credit get more benefits, and low credits lose benefits. But the worst part is that this can be being determined by AI-based surveillance without people's knowledge and consent.[§§]

There are differences in scope and scale. AI enables the collection of knowledge at an unprecedented scale and its use on many people simultaneously. There are differences in speed and individuation. AI systems can update their operating parameters in real-time and in highly individualised ways. Eventually, there are crucial differences within the degree of autonomy with which these systems operate, which may cause problems in how we assign legal liability and responsibility.

IV. LEGAL IMPLICATIONS

Law practices and abiding by them are non-negotiable parts of society and all institutions in a government. As much as the control over the protection of privacy lies in individual data subjects' hands, it also lies in the government's hands to implement legal controls such as strong regulations, heavy penalties on violations and liabilities, and an efficient workforce to implement these. The recent and speedy emergence of AI has made nations realise and reconsider their legislative controls and have started acting rigorously and diligently towards AI regulations. Following are few challenges that the legislators face during the making of these laws. User awareness and lack of specialists in legislative bodies create an additional burden.[***]

1. Personal Information

Numerous pieces of data security law ensure only personal data protection. In this sense, defining what constitutes 'personal information' acts as a watchman to the lawful assurances offered to people. The definition of personal data can change between jurisdictions, and it also advances alongside legal and societal standards, norms and cultures. Modern innovations can moreover alter the scope of personal data as unused types of data are created. In common parlance, the concept of personal data depends on the thought of identifiability - whether or not a person's identity can be sensibly found out from that data. In any case, the differentiation between what is and isn't considered to be 'personal' is being challenged by the expanding capacity to merge and coordinate information to people. In coming times, as the amount of collected data increases and technologies for preparing and processing it progress, it gets to be progressively troublesome to evaluate whether a given piece of information is 'identifiable'. AI can make data that are otherwise difficult to gather or does not as of now exist. This implies data being collected and utilized may exceed what is disclosed initially by a person. Gathering data in this manner raises concerns that whether it is worthy to gather personal data about a person who has chosen not to reveal it. Many data specialists propose this thought that there's a got to be a shift from seeing data in binary form to secure it in an AI environment.

2. Collection, Purpose and Use

OECD Guidelines[†††] lay down three strong pillars for information privacy, known as the triad of information privacy. First, data collection, secondly, the purpose for which the data was collected and thirdly, the limited use of the data so collected. The data collection should be done in a limited and need-based manner, meaning only what is required and necessary for an algorithm and related functions to work should be collected, with due knowledge or consent of the person whose data is being collected. Similarly, data should be collected for a specified purpose only, which must be iterated to the individual at the time of collection of their data, and they should retain the right to proceed with such data collection or not. After the limited collection of data for a specified purpose, the use of data should be limited for the sole purpose it was collected and iterated to the individual. Variations can only be made for an authoritative, legal and consensual basis. All three information privacy pillars in minimisation of data collected and used. However, AI creates a challenge for the implementation of all three.

[§§] Ross Anderson, *The Panopticon is Already Here*, (The Atlantic, Sep 2020), https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/ accessed 4 Feb 2021.

[***] Todd J. Burke & Scarlett Trazo, *Emerging Legal Issues in an AI-Driven World,* (Growling WLG, 2019), https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb accessed 4 Feb 2021.

[†††] Organisation of Economic Cooperation and Development, *Guidelines on the Protection of Privacy,* (OECD, 2013), https://piwik.pro/blog/oecd-guidelines-8-privacy-principles-to-live-by/#:~:text=Collected%20data%20must%20not%20be,at%20the%20time%20of%20collection.&text=Security%20Safeguards%3A,or%20disclosure%20of%20personal%20information. accessed 5 Feb 2021.

i. Collection Limitation

The inherent nature of a well-functioning AI system is the ingestion of a colossal amount of data. This data is required to feed into the algorithm for training purposes. It further creates data in the testing stage and then learns from the results, concluding in continuous cycles of unending related data. The advent of IoT complicates the matter even more. Connected smart devices around individuals, collect exchange and transfer information amongst themselves. This data is often freely given by users, but many a time, users are not aware of what data gets collected, creating a loophole for limiting the collection of data.

ii. Purpose Limitation

Organisations follow the purpose limitation approach by giving explanations through sending out notices and consent over-collection of data. Despite the nature of data collection, with AI and its capabilities, it is highly likely that the system would collect data that was not intended or collect more data than intended, thus creating a challenge towards specifying the purpose for which it was limited. Such collection of data would defy the purpose for which consent was sought from the individuals. And there's very little that an organisation can do to control this, apart from consistent monitoring and even then, there's always the possibility of false positives and human error. There will always remain some degree of risk involved with collecting such a massive amount of data. Policies and assessments can help in the accountability aspect, but that does not still solve the purpose limitation issue. A transparent, consented and reasonably exceptional system is therefore hard to implement.

iii. Use Limitation

Organisations are usually allowed to use data collected for secondary, internal or research purposes in such a manner that it is arguably reasonable and legal to do so. However, the use of data collected for training the AI model is a grey area currently, to be considered if its usage is justifiable or not. The high accuracy of AI models in predictions and pattern findings may be much greater than human counterparts. Still, on a downside, it also potentially impacts information that may or not lead to violation of a user's collected information.
Therefore, the need to distinguish between primary use and secondary use must be outlined at a planning stage to inculcate privacy at an early stage.

3. Transparency

The complexity of AI system also comes to the fact that not every algorithmic logic can be made accessible to the public or users for both business and functionality purposes. With AI, there also remains the problem of the 'black-box'[‡‡‡], that is, the evolving nature of the system, or to simply say how a machine 'thinks' can never be known. The lack of transparency leads to a loss of user trust and loyalty towards products. This lack of public awareness can become a barrier to data sharing, and organisations can miss out on tremendous opportunities to gain a competitive edge. This may even lead to loss of business in the industry, and almost all AI-based product organisations suffer from this issue. However, data protection laws still focus on making operations transparent by publishing policies, procedures, privacy notices, etc.

4. Consent

Consent is one of the most critical factors in securing privacy in an AI environment. The users should be made aware of their rights, nature of data collected, processed, exchanged, etc. Organisations must take consent from them regarding every process before moving ahead and acting on it. This means that users must understand what will happen to their data at every stage and that they retain the right to withhold the information up to maximum control. The European law makes it clear that such consent must not be ambiguous and must be an explicit affirmative action such as ticking 'I Agree' or 'Yes' boxes. Consent should be explicit at all stages and allow the users to have a clear choice. Now, since with AI, it is hard to keep track of the modifications over the user data. An approach towards graduated consent can be considered, where consent is taken stage-wise production of AI model. However, this is still debatable because it puts a heavy backlog on the efficiency of AI systems.

5. Discrimination

A study consisting of focus groups and telephonic interviews was conducted in the year 2013. The participants found out that widespread spying activities were going on by the government, private institutions, and even criminals. It also revealed that the participant data was used against them in a discriminatory manner. For instance, those with mental or medical illness were given fewer employment opportunities than others. Similarly, a legal AI system used by the judiciary was found to discriminate criminal data based on their

[‡‡‡] "Black box AI is any artificial intelligence system whose inputs and operations are not visible to the user or another interested party. A black box, in a general sense, is an impenetrable system. The process is largely self-directed and is generally difficult for data scientists, programmers and users to interpret."

ethnicity, stating that given the past records, how likely a criminal is prone to commit the same offence twice, affecting their penalty, lock-up time and bail procedure.

V. UNRAVELLING AI BASED SOCIO-LEGAL IMPACTS ON PRIVACY

Securing privacy and implementing measures can be done on three significant aspects that have been studied throughout the paper:

1. Legislation Controls

Good governance and having an overarching view on the functioning of data protection laws are strong measures to ensure that organisation and governments are kept under check and there is no misuse or violation of power by one against the other. A few shortcomings are listed below that make it difficult for the implementation of protection of privacy in the AI era through the use of legal mechanisms:

a. The creation, maintenance and implementation of privacy on artificial intelligence-based technology cannot be covered by one country or even one jurisdiction. It is an evolving subject, and therefore cross-border governance or establishing industry-wide best practices is difficult to carry out.

b. Despite existing legal regulations, it is difficult to identify the actual ownership and responsibility of protecting data. Modification, deletion, storage become confusing when data is collected over many data subjects and more so when there is an exchange or transfer of information across nations.

c. Good governance regulations come from an in-depth understanding of the subject matter. Now since AI is an emerging field and especially how its various applications speedily move into daily lifestyle, the study and research of it remain in the hands of very few across the globe, and the merge of law and technology is still a less discovered field in terms of both academics and career option.

d. It is difficult to strike a balance between how much and what all can be regulated. Absolute administrative power over the technology gives rises of the power being corrupted, whereas the lack of it leads to many loopholes for law-breakers to find and expose.

2. Organisational Controls

There are many controls that an organisation can inculcate at the development and production stage of any new algorithm. These steps can also include the legal aspects of checking through any new piece of data or a compliance checklist. Organisations can approach the security point of data privacy by looking at the risks it creates and devising a mechanism that holds strong liability and accountability of any discrimination in the personal data processing. Following are critical aspects of implementing the same:

a. Transparency

Organisations can implement disclosing of the algorithmic programming to provide transparency to the users in terms of how their data gets processed. Alongside this, the implementation of policies, procedures, and security standards across the organisation helps shape the organisation's security backbone by holding them accountable for every measure they put in place or that they do not. Moreover, privacy transparency would focus on what data is collected, how it is used, transferred and protected, internally and externally. The control level would also vary with the nature of the information collected, for instance, whether it was personally identifiable information, sensitive information or electronic health records.

b. Explainability

Where transparency gives users a prospective insight into the functioning of the algorithm, explainability works towards making the algorithm secure in a retrospective manner, which is at the stage of designing and planning. The European Law takes this approach in cases of breaches, violations or user rights requests, allowing the user or victim to view the logic behind the functioning of the algorithm that was under the operation of automated actions. This measure makes sure that there is a human intervention in automation that checks the false negatives and anomalies. The principle of explainability can be implemented by way of following three steps:

i. Recognising algorithmic logic
ii. Breaking down specific logics in algorithm
iii. A pipeline method for human intervention in algorithmic logic

Explainability removes the difficulty of reverse engineering in machine learning algorithms, and the inclusion of the human aspect makes it both legally sound and privacy-oriented.[§§§]

[§§§] Jonathan Johnson, *Machine Learning: Interpretability versus Explanability*, (BMC Blogs, 16 July 2020), https://www.bmc.com/blogs/machine-learning-interpretability-vs-explainability/ accessed 6 Feb 2021.

c. Risk Assessment

Risk assessment is the structural analysis of the threats and vulnerabilities that come out from a privacy related asset and the likelihood and impact of that asset being compromised. Risk assessment on AI-based algorithms allows the study of system preferences in the designing stage regarding the data involved. For a successful risk assessment, the degree of risk assessed should be appropriately balanced against the assets and nature of data assessed. Assessment of AI-related data becomes highly quantitative, creating an equal number of complexities and accuracy.[****]

d. Data Protection Impact Assessment

One of the key essential features that came off from the European Law, GDPR[††††], was the advent of DPIA, data protection impact assessment. This puts an obligation on any organisation proposing to be the data controller to conduct and document an impact assessment before processing the collected data. The severity of assessment increase with the likelihood of high risk involved as to subjects rights and data. However, the DPIA is not mandatory, but the controls implemented should justify the assessment's absence. This process is periodic and needs to be carried out at least once every three years.[‡‡‡‡]

e. Audits

Legal recourses are not always retrospective and do not always cover all aspects of security and privacy. However, internal and external audits from experienced and certified individuals or authorities can help in having accountability in place as to the privacy issues of AI and related products. These are highly thorough and brings out any existing or future vulnerabilities in the system. Awareness across the organisation, training programs and internal assessments are few ways that audit findings can be implemented and continually improved. [§§§§]

3. Public-level Controls

On a more ground level, for the public at large, the following measures are identified that provide awareness on how to protect their privacy and prevent the creation of huge amount of digital footprints by responsible use of technology that is all around them:

a. Browse through Anonymous Networks

Browsing history becomes a huge database by collecting information from cookies, cache files, metatags and session data. It is possible that despite the deletion of these, they get stored in an unencrypted manner over some servers because of the weak security measures of the network being used. Therefore networks like Freenet, Tor or I2P are advised for users to connect safely over the internet. These networks allow end-to-end encryption, meaning the integrity of search and conversations is not compromised by any third party.

b. Use Open-Source Web Browsers or Search Engines

Users often use browsers based on convenience and user-interface, leaving behind the aspect of privacy. Browser like Firefox or search engine DuckDuckGo is advised over Chrome or Google respectively to keep security intact because these platforms are easy to self-audit for any vulnerabilities and do not collect or track user activities performed over time.

c. Use Open-Source Operating Systems

Operating systems makes a ton of difference in security. Manufacturers like Apple and Microsoft are often prone to backdoor or man-in-the-middle attacks and collect user data through the metadata. However, many Linux based distribution packages are freely available over the internet that can be used to protect data and secure privacy.

d. Use Android Cell Phones

While purchasing mobile mobiles, an android based operating system should be preferred over that of Microsoft or Apple because, however, the risk still exists with android OS, the counterparts have a higher risk towards malicious use of user data. Hardware and application require user input and their personal or private information

[****] Balu N. et al, *Artificial Intelligence: Risk Assessment and Considerations for the Future,* (International Journal of Computer Applications, March 2019), https://www.researchgate.net/publication/331790918_Artificial_Intelligence_Risk_Assessment_and_Considerations_for_the_Future accessed 7 Feb 2021.

[††††] Regulation (EU), 2016/679 (General Data Protection Regulation)

[‡‡‡‡] ICO, *Data Protection Impact Assessments and AI,* (ICO UK, 23 Oct 2019), https://ico.org.uk/about-the-ico/news-and-events/ai-blog-data-protection-impact-assessments-and-ai/ accessed 7 Feb 2021.

[§§§§] James Bone, *Auditing Artificial Intelligence: Planning an AI Audit Engagement,* (Corporate Compliance Insights, 27 July 2020), https://www.corporatecomplianceinsights.com/auditing-artificial-intelligence/ accessed 7 Feb 2021.

at the time of installation for the full functionality of the phone. Android systems still provide more transparency regarding the data collected, and the purpose limitation principle is kept in mind because of the open-source software.

Combining these measures will help strengthen the privacy be design approach and add multiple layers of security, accountability, liability, and legal obligations. Both correction and corrective actions can be brought out of these measures to improve upon them. Though not all automated and AI-based algorithms may turn consequential, the need to study risks, threats and vulnerabilities remain a priority.

VI. CONCLUSION AND SUGGESTIONS

Privacy is a pivotal part of a person's life. It has become challenging to protect privacy in this information age because people are not aware of their rights and the measures they can take to combat privacy violations. Advanced innovations such as AI have made significant commitments to numerous zones of life. The tremendous amounts of data that organisations are ready to accumulate and analyse through these devices permit people to handle social ills that already had no solutions. Unfortunately, these advances can be utilized against society by different social actors, from people to organizations, to government offices. Our misfortune of protection is fair, one illustration of how advances such as AI can work to human disservice. However, suppose people manage to understand these innovations and their effect on the lifestyle legitimately. People will secure the implies to guard themselves against abuse by using them with malicious intent.

Following suggestions are made to have an insight towards a way forward on protecting privacy in an artificially run intelligent society:

a. Development of regulatory sandboxes

The exponential use of digital services is pressurizing technologists to discover security building arrangements to reduce the common concerns on protection. The GDPR, among others, points at giving legitimate confirmations concerning the security of individual information, whereas an expanding number of systems, instruments, and applications demand personal information. On the one hand, laws and directions for ensuring protection, securing individual information and guaranteeing usable digital identities have never been so thorough. On the other hand, compliance with the GDPR and other pertinent data regulation remains challenging with today's dangerous landscape, making the risks of information breaches bigger than ever. Beyond technical solutions, which exist, another trade opportunity is opening up: Secure data storage environments (that will be portion of the individual, mechanical or even hybrid information platforms). These are digital environments that are topic-oriented, connected, and certified by the information assurance specialists, advertising the possibility to train calculations that have to be prepared on genuine information. Combined with such approaches, lessons learnt from past cases, and best practices help upgrade different industrial sectors. This would permit to bring Europe forward in making commerce from AI/ML taking into account technology that protects privacy by design.

b. Continued support for research, innovation and deployment of Privacy-Preserving Technologies

One of the most challenging issues recognized and broadly underlined by the stakeholders is that of adaptability. The main contention here is that the uptake of Privacy-Preserving Advances endures a bootstrapping issue: the more certain arrangements are utilized, the better they end up; but for companies and SMEs to begin using them, they got to be efficient (i.e., strong, verified, standardized, known within the industry etc.). Numerous sorts of arrangements arise from research and development communities in privacy designing. Inside privacy designing, measures can come from community-identified issues that develop amid the advancement of digital services; they can come from committed programs in which measures are pitched for known and existing social issues. They can start from requests posed by the direction of a certain digital technology. Continuous effort should be made to create training, instructional exercises and tool support (e.g. libraries, open-source components, testbeds) and to use these in tutorials in educative form. Bringing out and following industry-wide best practices for putting in play privacy by design technologies in every sector would be a good way forward towards the uptake of these.

c. Support and contribute to the formation of technical standards for preserving the privacy

Diverse applications of big data innovations lead to diverse sorts of potential threats and risks that require distinctive treatments and technological measures. The work done by ISO standardisation bodies and others that handle the challenge of classification of technologies is pivotal in understanding, forming and prioritizing challenges and solutions within privacy designing. The sanitizations endeavours by projects mentioned earlier also push forward creating a common security language and semantics between machine and human language. This can be an essential step for automating compliance and for planning big data for AI. We

ought to work on maturity modelling and keep supporting endeavours to extend the improvement and execution of technological measures around privacy-preserving technologies.

Sound governance systems can promote great plan, structure and oversight of AI innovations and how they associate with privacy. By making an environment in which common rights and securities are revered, the direction can provoke the improvement of automated frameworks supported by data security, steady with a Privacy by Design approach to security assurance. Security governance cannot be accomplished exclusively through top-down control from controllers; those who control the information, and those building the innovation, should themselves be included within the plan of privacy improving frameworks.

REFERENCES

Statute

[1]. General Data Protection Regulation, Regulation (EU), 2016/679

Book

[2]. Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, (1st Ed, Oxford University Press, 2014)

e-Book

[3]. Information Commissioner's Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (ICO UK, Sep 2017), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf accessed 5 Feb 2021.

[4]. Website Sources

[5]. Rick Falkvinge, *Our Seven Privacies: The Many Important Facets of Privacy*, (Privacy News Online, 13 Nov 2013), https://www.privateinternetaccess.com/blog/our-seven-privacies-the-many-important-facets-of-privacy/#:~:text=There%20are%20seven%20distinct%20important,invade%20it%20without%20your%20consent. Accessed 4 Feb 2021.

[6]. Michael Deans, Towards Data Science, *AI and the Future of Privacy*, (Towards Data Science, 5 Sep 2018), https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4 accessed 4 Feb 2021.

[7]. Elena Boldyreva, *Cambridge Analytica: Ethics and Online Manipulation With Decision-Making Process*, (St. Petersberg Polytechnic University, Dec 2018), https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process accessed Feb 4 2021.

[8]. Nick Statt, *Clearview AI to stop selling controversial facial recognition app to private companies*, (The Verge, 7 May 2020), https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law accessed 4 Feb 2021.

[9]. Jacob Kastrenakes, *Controversial deepfake app DeepNude shuts down hours after being exposed*, (The Verge, 27 June 2019), https://www.theverge.com/2019/6/27/18761496/deepnude-shuts-down-deepfake-nude-ai-app-women accessed 4 Feb 2021.

[10]. Ross Anderson, *The Panopticon is Already Here*, (The Atlantic, Sep 2020), https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/ accessed 4 Feb 2021.

[11]. Todd J. Burke & Scarlett Trazo, *Emerging Legal Issues in an AI-Driven World*, (Growling WLG, 2019), https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb accessed 4 Feb 2021.

[12]. Organisation of Economic Cooperation and Development, *Guidelines on the Protection of Privacy*, (OECD, 2013), https://piwik.pro/blog/oecd-guidelines-8-privacy-principles-to-live-by/#:~:text=Collected%20data%20must%20not%20be,at%20the%20time%20of%20collection.&text=Security%20Safeguards%3A,or%20disclosure%20of%20personal%20information. accessed 5 Feb 2021.

[13]. Astha Oriel, *Fighting Discrimination in AI Using Legal and Statistical Precedents*, (Analytics Insight, 28 Oct 2020), https://www.analyticsinsight.net/fighting-discrimination-in-ai-using-legal-and-statistical-precedents/ accessed 5 Feb 2021.

[14]. Jonathan Johnson, *Machine Learning: Interpretability versus Explainability*, (BMC Blogs, 16 July 2020), https://www.bmc.com/blogs/machine-learning-interpretability-vs-explainability/ accessed 6 Feb 2021.

[15]. Balu N. et al., *Artificial Intelligence: Risk Assessment and Considerations for the Future*, (International Journal of Computer Applications, March 2019), https://www.researchgate.net/publication/331790918_Artificial_Intelligence_Risk_Assessment_and_Considerations_for_the_Future accessed 7 Feb 2021.

[16]. ICO, *Data Protection Impact Assessments and AI*, (ICO UK, 23 Oct 2019), https://ico.org.uk/about-the-ico/news-and-events/ai-blog-data-protection-impact-assessments-and-ai/ accessed 7 Feb 2021.

[17]. James Bone, *Auditing Artificial Intelligence: Planning an AI Audit Engagement*, (Corporate Compliance Insights, 27 July 2020), https://www.corporatecomplianceinsights.com/auditing-artificial-intelligence/ accessed 7 Feb 2021.

Mayank Tiwari, et. al. "Socio-legal Impact on Privacy in AI-Driven World."*IOSR Journal of Humanities and Social Science (IOSR-JHSS)*, 26(04), 2021, pp. 39-48.