PRIVACY IN THE AGEOF AI

BY ISHITA VERMA
STUDENT AT UPES, DEHRADUN

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

One of the many contemporary methods for achieving machine intelligence on par with human intelligence is artificial intelligence (AI). Other strategies include organizing networks (like the Internet) into a collective intelligence and simulating the brain, biological cognition, and human-computer interfaces. Artificial intelligence is one of these technologies that has made significant progress and is widely used in daily life. The creation of intelligent entities is the focus of artificial intelligence research, which has many applications in a variety of domains, including games, driving, and mathematical theorems.[1]

A subfield of computer science is artificial intelligence. It aims to comprehend the nature of intelligence and create a new class of intelligent machine capable of thinking like a human. Since the beginning of artificial intelligence, the theory and its application have grown increasingly complex, with a never-ending scope. It is conceivable that artificial intelligence will eventually produce technological products that serve as the "container" for human intelligence. Artificial intelligence is capable of simulating human consciousness and thought processes. Though it can think like humans and eventually outsmart them, artificial intelligence is not the same as human intelligence. Everybody in life has a secret that they would prefer to keep to themselves and that has nothing to do with other people's rightful interests. This secret, such as personal privacy, diaries, photo albums, lifestyle habits, communication confidentiality, physical defects, and so forth, is referred to as privacy in law. To keep one's secrets private from other people is a personal right. We refer to this right as the right to privacy.[2] However, personal privacy has turned into a commodity in the Internet society. Within the shadows of the Internet, individual privacy is identified and traded. Because of this, it is now crucial to protect privacy from an IT and legal standpoint.

---

[1] Karl Manheim, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 Yale J.L. & Tech. (2019).

[2] Zhizong Chen, *Privacy Protection Technology in the Age of A.I.*, 750 IOP Conference Series: Materials Science and Engineering (2020).

CHAPTER 2
UNDERSTANDING AI: A COMPREHENSIVE OVERVIEW

2.1 INTRODUCTION TO AI

The rules of reasoning are intended to be followed by a logically reasoning system. These laws include the identity principle, the law of excluded means, and the law of contradiction. These systems are designed to construct sound argumentative structures logically from a sound premise. Stated differently, these are systems built to strictly apply logic to solve issues, which poses some challenges. Creating meaningful logical semantics from informal knowledge (such as that which is derived from unstructured data) is one such challenge. Another is how to make information decisions based on priority when there is an abundance of information. This results in computational time constraints when determining what data should be taken into consideration, especially when there is uncertainty.[3]

Artificial intelligence, which depends on computer programmes with human-like feelings, thoughts, abilities to learn, actions, and adaptations, is a type of "intelligent computing".[4] It mimics human thought processes, which makes it "intelligent." Six Because it depends more on computer processing of information than on biology, it is "artificial." The enormous amounts of data that can be analysed for meaning and the exponential growth of computer processing and storage are the main sources of AI's growing power.[5] Today's robotics and computing powerhouses make many of the science-fiction predictions of the past seem quaint in comparison. AI capabilities will advance more quickly than we can anticipate or prepare for, thanks to the impending arrival of quantum computing. [6]

2.2 UNDERSTANDING THE FUCTION OF AI

Artificial Intelligence (AI) has its origins in the early 1900s, when innovators such as Alan Turing established the foundation for computing devices that could execute tasks that were previously thought to be exclusive to human intellect.[7] Big Data, cloud computing, and powerful computing resources have all contributed to the explosive growth of AI research and development in recent decades. The development of AI has greatly increased the potential for advancing and defending human rights. On the one hand, AI-powered apps advance inclusion and equality by enhancing access to healthcare and education in

---

[3] Cheng-Kai Liu,Ching-Yen Tu,Hsing-Ru Lin,Ko-Ting Cheng. *Asymmetrical transmission windows for dailyprivacy protection using cholesteric liquid crystals[J]*. Optics and Laser Technology,2020,121.

[4] Scientists may call this “computational intelligence,” which Al is subset of.

[5] FUTURE of Artificial Intelligence Act, H.R. 4625, 115th Cong. 3 (2017)

[6] *Algorithms Based on Brains Make For Better Networks*, NEUROSCIENCE NEWS (July 17, 2015), https://neurosciencenews.com/neuroscience-network-algorithms-2263.

[7] Wei Kong,Jian Shen,Pandi Vijayakumar,Youngju Cho,Victor Chang. *A practical group blind signature schemefor privacy protection in smart grid[J]*. Journal of Parallel and Distributed Computing,2020,136.

underprivileged areas.[8] Conversely, the predictive powers of AI hold the potential to transform the criminal justice system, minimize injustices, and guarantee impartial trials. Nonetheless, it's important to remember the drawbacks of AI development: Human rights are seriously threatened by algorithmic biases and discriminatory practices in AI systems, which also lead to structural inequality. Furthermore, there are now significant privacy and data protection concerns due to the relentless pursuit of data-driven knowledge. Large-scale personal data collection by AI algorithms raises the possibility of exploitation and surveillance.[9]

Machine learning is a tool used in AI system design and implementation that mainly relies on statistical techniques to accomplish its objectives. Machine learning allows an AI system to learn from experience, while sensors are used by the system to sense its surroundings and actuators are used to carry out actions. Important issues in AI are being resolved by machine learning research, including how to improve systems autonomously and which computational and statistical information laws apply to learning systems. A model that predicts future outcomes based on new inputs is produced by a machine learning system through a training process. Usually, reinforcement learning, unsupervised learning, semi-supervised learning, or supervised learning are used to build machine learning models. More sophisticated models that process ever-increasing volumes of data are among the latest developments in machine learning.[10]

[8] Shahana Rayhan, *AI Odyssey: Unraveling the Past, Mastering the Present, and Charting the Future of Artificial Intelligence*, ResearchGate (2023).

[9] Rajan Rayhan, *AI and Human Rights: Balancing Privacy and Innovation in the Digital Age*, Research Gate(2023).

[10] M. I Jordan, *Machine Learning: Trends Perspectives and Prospects*, 349 Science 255-260 (2015).

CHAPTER 3
CHALLENGES OF AI: ETHICS AND PRIVACY

3.1 CONCERNS ABOUT AI

The application of artificial intelligence (AI) on par with human intelligence raises a variety of public concerns, from economic instability to apocalyptic outcomes, even though it also has advantages like accelerating technological development. The public's concern over privacy violations by AI-enabled devices is growing, particularly in light of the introduction of personal assistants like Google Home and Amazon Alexa. Public acceptance of AI[11] is not aided by stories and articles about these devices spying on people and recording speech patterns.

Deep neural networks have been demonstrated to be able to classify a person's sexual orientation with 91% accuracy based only on their facial features. This technology offers a way for someone to reveal their sexual orientation, something they might not otherwise want to reveal, which has direct implications for privacy. More importantly, sexual orientation becomes a matter of life and death in oppressive regimes, and the oppressed are far more vulnerable to the risks posed by AI developments. Furthermore, there are direct privacy implications for the features used in practice and the training data. [12]

The digital services we use and the physical devices we own are becoming more and more integrated with artificial intelligence (AI). In order to provide users with personalised content and enhanced features like relevant search results, content that users like, and people they know, the most popular digital services, including search (Google, Bing), music (Spotify, YouTube Music), entertainment (Netflix, YouTube), and social media (Facebook, Instagram, Twitter), already rely on artificial intelligence (AI) or machine learning (ML). Additionally, artificial intelligence (AI) improves a variety of tangible items that we currently possess (or may acquire), such as smart speakers like the Google Hub and Amazon Echo. These devices use natural language processing to recognise and comprehend speech and carry out commands, such as controlling lights, temperature, or adding groceries to the shopping list. Using AI to deliver highly personalized experiences benefits both users and providers: users gain positive engagement with these platforms and providers gain engaged users who spend more time using their services.[13]

The ability of artificial intelligence to surpass human intelligence is the subject of lively debate. The Turing Test is an experiment in which a human interviewer, in a blind conversation, is unable to distinguish between human-generated and computer-generated natural language responses. Futurologist Ray Kurzweil has

---

[11] Geoffrey A Fowler, *Alexa has been eavesdropping on you this whole time*, The Washington Post (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/.

[12] J Curzon, *Privacy and Artificial Intelligence*, 2 IEEE Transactions on Artificial Intelligence (2021).

[13] Martin Abadi, *Deep Learning With Differential Privacy*, ACM SIGSAC Conference on Computer and Communications Security 308-318 (2016).

predicted that the Turing test willbe passed in 2029. Until then, we will remain in the era of Narrow Artificial Intelligence (NAAI) or Weak Al, in which specialized computer programs outperform humans in certain tasks such as games of skill and text analysis. Included in ANI is cognitive computing, where machines help people with tasks like reading X-rays for radiologists, processing stockbrokers' transactions, and helping lawyers draft contracts.[14]

3.2 AI-RELATED PRIVACY ISSUES

AI technology increases the ability to collect, analyze and aggregate incredibly large amountsof data from multiple sources to an unprecedented level. What's more, this type of technologyis now widely accessible to all types of people and organizations worldwide. Although information technologies have already had an impact on privacy, this new capability greatly increases the potential for privacy breaches that were not previously considered.

A common method of assessing privacy breaches is to carry out a Privacy Impact Assessment(PIA). Performing an effective privacy impact assessment is itself an evolving area of research, in which current methodologies and frameworks can be borrowed and applied to AI. Guidelines like the ones in recommend beginning a PIA as soon as feasible and include thorough methodology. The guidelines issued by the CNIL propose an approach to privacy protection factor assessment that is compliance-based and considers the fundamental principles of data subject rights in order to identify and mitigate risks.[15] Preliminary analysis, project analysis, data protection analysis, and report preparation are the stages of a data protection impact assessment. Here, we concentrate on the privacy analysis stage and its potential applications to AI in general.

3.2.1 AI CHALLENGES AND THREATS TO HUMAN RIGHTS

As artificial intelligence becomes more pervasive in our daily lives, worries about potential violations of human rights have increased. Biassed historical data can be used to justify discrimination, which can result in unfair treatment and decisions that are not equitable, ranging from hiring procedures to credit allocation. Furthermore, severe data protection concerns have been raised by AI's voracious appetite for data. People are becoming more and more susceptible to data mining and surveillance as AI systems gather, process, and analyse enormous volumes of personal data. The right to privacy and autonomy is consequently threatened by the commercialization of personal data.

3.2.2 THE INTERNET OF THINGS

[14] Rajan Rayhan, *AI and Human Rights: Balancing Privacy and Innovation in the Digital Age*, Research Gate(2023).

[15] J. A Perez, *Artificial Intelligence and Robotics*, ResearchGate (2018).

The ability of machines to access data is what gives artificial intelligence its power. In essence, artificial intelligence crushes data. Al can therefore respond to requests and carry out tasks more effectively the more information there is available on a subject or the larger the accessible data set. An ecosystem of electronic sensors found in our bodies, homes, workplaces, cars, and public areas is known as the Internet of Things, or "IoT."[16] Any real or manufactured object that has been given an IP address and can send data over a network without requiring human-to-human or human-to-computer interaction is referred to as a "object." If the human brain is Al, then the Internet of Things is the human body, gathering information about senses (tact, vision, and sound). IoT devices gather unprocessed data about people engaging in physical and other activities. Large-scale data collection, archiving, and analysis have been made easier by these gadgets.[17]

3.2.2 AI INTRUSION INTO PRIVACY

AI has the ability to fully integrate the privacy of any Internet user with corporate data through non-standard integration data mining technology and personal network behavioural profiling, even if the user has never given their entire personal information to a network platform or institution.[18] Information discovery, information integration, attribute analysis, and user portrait are its four primary components. AI-integrated privacy data can be sold directly to criminals for illicit use, or it can be used for a variety of promotional campaigns.

3.2.3 DATA COLLECTION AND USE BY AI TECHNOLOGIES

The way artificial intelligence technology gathers and processes data is one of its most significant ramifications. AI systems are built to analyse vast amounts of data in order to learn and get better. As a result, concerns regarding data protection and privacy are raised by the fact that AI systems are continuously collecting more and more personal data. To see how our data (articles, photos, videos, etc.) is used, frequently without our permission, we only need to look at a variety of creative AI tools like ChatGPT, Stable Diffusion, or others that are still in development.

Above all, there is sometimes a lack of transparency in how AI systems use personal data. People may find it challenging to comprehend how their data is used to make decisions that have an impact on them due to the complexity of the algorithms used in AI systems. Unease and mistrust of AI systems can result from a lack

---

[16] Jonathan Shaw, *Artificial Intelligence and Ethics*, HARV.MAG https://www.harvardmagazine.com/2019/01/artificial-intelligence-limitations.

[17] Awais Ahmad, *A Cluster-Based Data Fusion Technique to Analyze Big Data in Wireless Multi-Sensor System*, ResearchGate (2017).

[18] Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 18, 2023), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198.

of transparency. It's critical that businesses and organisations utilising AI technology take security measures to safeguard individual privacy in order to allay these worries. These include putting in place strict data security procedures, making sure that data is only used for what it was meant to be used for, and creating AI systems that follow moral guidelines.

Of course, it's critical that personal data used by AI systems be used transparently. People need to be in charge of and able to comprehend how their data is used. This includes the option to ask for the removal of data and to object to its collection. By doing this, we can influence a future in which AI technologies are applied to advance society while safeguarding personal information.

3.2.4 THE USE OF AI IN SURVEILLANCE

Of course, it's critical that personal data used by AI systems be used transparently. People need to be in charge of and able to comprehend how their data is used. This includes the option to ask for the removal of data and to object to its collection. By doing this, we can influence a future in which AI technologies are applied to advance society while safeguarding personal information.

Surveillance is one of the most contentious applications of AI technology. While AI-powered surveillance systems hold great promise for improving security and law enforcement, they also seriously jeopardise people's privacy and liberties.

Algorithms are used by AI-powered surveillance systems to evaluate vast volumes of data from numerous sources, including cameras, social media, and other online sources. This makes it possible for security and law enforcement organisations to monitor people and anticipate criminal activity before it happens. Artificial intelligence-powered surveillance systems raise issues with privacy and civil liberties, even though they may seem like a useful tool in the fight against crime and terrorism. Some who oppose these systems claim that they can be used to track and manipulate people, possibly resulting in the loss of civil liberties and rights.

The use of artificial intelligence-powered surveillance systems is not always transparent, which only serves to exacerbate the situation. People may find it challenging to understand why or when they are being watched. People may become uneasy and lose faith in the police and security services as a result of this lack of transparency. Artificial intelligence-based surveillance systems must be used under tight regulation and control in order to allay these worries. This calls for the creation of independent control and review mechanisms in addition to explicit policies and procedures for the use of these systems.

People should have access to information about the collection and use of their data, and law enforcement and security organisations should be open and honest about the use of these systems and their timing. The integration of artificial intelligence-powered surveillance systems has surely benefited law enforcement and security organisations greatly. Recognising the possible threats these systems pose to our fundamental

liberties and rights is crucial, though. To ensure the protection of privacy and individual freedoms, regulators must address a number of issues, including a lack of transparency and the possibility of discrimination. Putting strong laws and oversight in place is crucial to ensuring that AI technologies are applied for the good of society in the future without infringing on peoples' rights and liberties. Ensuring transparency in the implementation of AI-based surveillance systems through the establishment of clear policies and procedures is crucial. To guarantee accountability, independent monitoring and review procedures should also be established.

CHAPTER 4

PRIVACY AND DATA PROTECTION IN THE AGE OF ARTIFICIAL INTELLIGENCE

AI and privacy interact in a way that is intricate and multidimensional. The implications of AI for individual and collective privacy are significant in this era of data-driven decision-making, and it is critical for both the public and policymakers to understand these implications. The issue of privacy has grown more complicated in the AI era. The amount of personal data that governments and businesses are gathering and analysing makes it more vulnerable than ever.

These problems include unauthorised data collection, which can jeopardise sensitive personal information and expose people to cyberattacks, and intrusive surveillance, which can weaken people's sense of autonomy and worsen power disparities. The power of BigTech companies, which possess enormous amounts of data and have significant influence over its collection, analysis, and use, frequently makes these issues worse.

The rapid expansion of data-driven technologies and artificial intelligence's capacity to handle enormous amounts of data present significant obstacles to data security and privacy. AI systems raise the risk of unauthorised access and privacy violations as they gather data from various sources. In the AI era, effective data anonymization techniques and making sure AI algorithms prioritise data minimization are two strategies for balancing innovation and data protection. Furthermore, incorporating data protection guidelines into the design process can encourage the creation of AI systems that are fundamentally sensitive to individuals' right to privacy.

There is no guarantee that AI will not harm consumers, even if we are able to strictly protect all data and restrict its use. Frequently, predictive algorithms presume that hidden information about a customer's gender, income, residence, sexual orientation, political preferences, or willingness to pay can be discovered.

However, the "truth" that needs to be learned occasionally changes and is influenced by outside factors. In this way, although the algorithm's goal may be to discover the truth, it ultimately defines it. This can be harmful because algorithm creators use them to further their personal goals, which may not align with those of customers. Examples of these goals include pursuing financial gain, gaining political power, or advancing cultural change. The controversy surrounding the distribution of Russian-sponsored contributions on social media during the 2016 US presidential election has already brought attention to the risk posed by misleading algorithms.[19] Legislators voiced concerns during congressional hearings on

[19] Roberrt S. Mueller, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*(March 2019), https://www.justice.gov/storage/report.pdf. A searchable version is available at Read the Muller Report, N.Y. TIMES (April 18, 2019), https://www.nytimes.com/interactive/2019/04/18/us/politics/mueller- report-document.html.

October 31 and November 1, 2017, regarding Facebook, Twitter, and Google's potential impact on their ability to identify or restrict misinformation from problematic users due to their reliance on advertising revenue from a large user base.

CHAPTER 5
PRIVACY PROTECTION LAWS AROUND THE WORLD

5.1 PRIVACY PROTECTION IN THE USA

Some of the biggest and most cutting-edge technology and data companies in the world are based in the United States. Experts blame their dominance in the global market on the lack of extensive federal privacy and personal data protection regulations. The USA, on the other hand, employs a "sectoral approach" that consists of a patchwork of federal laws that are sector-specific, frequently enforced by various agencies, and that establish varying standards.

On the other hand, the European Union (EU) and numerous other developed nations take a comprehensive approach, enacting a single law that consistently governs the gathering, use, and disclosure of data in all industries. For instance, all entities that are "established" in the EU, offer goods or services there, or provide services to EU citizens are subject to the EU's General Data Protection Regulation (GDPR), which is a general regulation that applies to all sectors and member states. [20]

Initially, many US businesses favoured a sectoral approach so they could customise the regulations to meet their unique requirements. Although there is some truth to this model, it also helps industry pressures, regulatory capture, and privacy violations that frequently evade the regulatory net. A patchwork of state and federal laws that "overlap, intersect, and contradict each other" has been produced by the sectoral approach.

5.2 EUROPEAN PRIVACY LEGISLATION

The General Data Protection Regulation (GDPR) of the European Union, which went into effect on May 25, 2018, has had significant effects, in contrast to the US regulatory framework. Administrative fines for violators can reach twenty million euros, or four percent of an organization's yearly global revenue, whichever is greater.311 Consequently, tech behemoths like Google have been compelled to alter their operations in reaction to the GDPR's penalties.[21]

Europe's experiences during World War II can help to explain some of the differences between US and EU privacy policies. Many nations realised that in order to sustain democratic institutions, fundamental

---

[20] Mark Rotenberg, *On International Privacy: A Path Forward for US and Europe*, HARV. INT'L REV. (June 15,2014), http://hir.harvard.edu/article/?a=5815.

[21] Regulation (EU) 2016/679 of European Parliament and of Council of 27 April 2016 on protection of thenatural person(s) with regard to processing of the personal data and on free movement of data.

human rights had to be upheld following the war and the founding of the UN. Privacy was recognised as a fundamental human right in 1948 by the Universal Declaration of Human Rights (UDHR), which established certain principles. The right to privacy is broadly protected by Article 19. Article 19 offers extensive safeguards for the right to free speech. The GDPR was drafted by the EU with direct application to each and every member state. The goal was to develop a logical framework for data protection that would be strictly enforced and give people more rights.[22] The GDPR provides people more control over their data, which boosts confidence in the online world and digital economy. The GDPR frequently emphasises accountability, transparency, and control.

5.3 THE INDIAN PERSPECTIVE

India does not currently have any laws specifically governing AI. The executive agency for AI-related policies is the Ministry of Electronics and Information Technology (MEITY), which has established committees to draft an AI policy framework. Seven principles—privacy and security, transparency, accountability, inclusion and nondiscrimination, safety and dependability, fairness, and the preservation and advancement of positive human values—have been formulated by the Niti Ayog for responsible AI.[23] It is the constitutional duty of the Supreme Court and the High Courts to protect fundamental rights, such as the right to privacy. The Information Technology Act and its implementing regulations have been India's main privacy laws up until this point.

The technology sector, especially those involved in AI and ML, has been forced to reconsider how they conduct business and handle data due to the Digital Personal Data Generation Bill 2023, which was submitted to the Lok Sabha in its current form. As legal specialists have noted, no business can continue to afford to handle data carelessly. AI developers and companies therefore have a great deal of work ahead of them. The logic behind developing and refining AI models to produce chatbots or other services has been impacted by the bill. AI developers and development studios will now need to obtain permissions for many things, including where and how data is obtained as well as what happens to data after it has been used to train AI models that all required compliance rules have been lawfully implemented.

With the impending passage of the Digital Personal Data Protection Act (DPDP Act) 2023, India will soon have a brand-new data protection legislation. By outlining compliance requirements for data fiduciaries— those who gather and handle data digitally—as opposed to data principals—those who possess the data—the Act offers a safeguard. At a time when the use of AI-based apps that have been

[22] Mark Rotenberg, *On International Privacy: A Path Forward for US and Europe*, HARV. INT'L REV. (June 15,2014), http://hir.harvard.edu/article/?a=5815.

[23] Niti Aayog, *Adopting the Framework: A Use Case Approach on Facial Recognition Technology*, NITI AAYOG (Nov. 1, 2022), https://www.niti.gov.in/.

trained on copious amounts of personal data is growing in popularity, the law has been a huge relief. India's Digital Personal Data Protection Act 2023 has various flaws that it neglects to address, despite the relief that personal data must be gathered and processed in compliance with the law.

First off, as long as the objective is legitimate, there are no rules governing the collection and use of data. Administrators are permitted by law to gather data for any legitimate purpose as long as it is done so. This implies that, with the exception of children, algorithms that monitor user preferences and adverts that take advantage of a user's private information and online activity (dark patterns) are free to be used.[24]
Second, for the law to be successful, the people of the nation must be aware of their rights and be able to use the Data Protection Act's complaints process to enforce them.

The DPA and other authorities are not required by law to notify the public of their rights under the GDPR or to verify that administrators and data controllers are complying with the regulations. Furthermore, there is no duty to proactively reduce damages. Given these details, the GDPR law, despite its good intentions, lacks the necessary enforcement power.[25] When the DPDP Act's provisions are contested in court, many of these ambiguities ought to be clarified. It is hoped that MEITY will proactively change the law or publish regulations to make the matter clear in the interim.

5.4 THE EU AI ACT

The first comprehensive artificial intelligence (AI) regulation by a major regulator worldwide is the proposed European AI Act. Applications of AI are divided into three risk categories by the Act. Initially, programmes and platforms that pose an unacceptable risk are prohibited. Second, certain legal requirements apply to high-risk applications. Finally, most applications that aren't specifically prohibited or labelled as high-risk are free of regulation. Similar to the EU's 2018 General Data Protection Regulation (GDPR), the EU AI Act may establish a worldwide standard that determines the degree to which AI improves rather than negatively impacts your life, wherever you may be. By guaranteeing that AI systems uphold fundamental rights, safety, and ethical principles, as well as by addressing the risks associated with extremely potent and significant AI models, the new regulations aim to encourage trustworthy AI in Europe and beyond.[26]

Sometimes, it is impossible to determine the reasoning behind an AI system's decision, prediction, or

[24] Nivedita Krishna, *The Digital Personal Data Protection Act, 2023: Some relief but many questions*, TIMESOF INDIA (Oct. 29, 2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the- digital-personal-data-protection-act- 2023-some-relief-but-many-questions/.

[25] Nivedita Krishna, *The Digital Personal Data Protection Act, 2023: Some relief but many questions*, TIMESOF INDIA (Oct. 29, 2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the- digital-personal-data-protection-act- 2023-some-relief-but-many-questions/.

[26] *Home*, EU Artificial Intelligence Act (Sept. 7, 2021), https://artificialintelligenceact.eu/.

action. As a result, it could be challenging to determine whether someone has suffered unjust disadvantage when applying for a public benefit programme or being hired. Even though there is some protection offered by current law, it is insufficient to handle the unique problems that AI systems may present.

The proposed rules will:

- address the risks that AI applications specifically create;
- ban AI practices that present unacceptably high risks;
- ascertain a list of applications deemed high-risk;
- impose precise specifications on AI systems in high-risk applications;
- specify particular responsibilities for high-risk AI application providers and deployers;
- require a complying assessment prior to deploying or commercialising a specific AI system;
- implement enforcement following the deployment of a specific AI system;
- create a national and European governance framework.

The Commission established the European AI Office in February 2024 to supervise the member states' implementation and enforcement of the AI Act. The Artificial Intelligence Act will go into effect twenty days after it is published in the Official Journal, and it will be fully applicable two years later, with the following exceptions: six months will pass before prohibitions become effective, twelve months will pass before governance rules and obligations for general-purpose AI models become applicable, and thirty-six months will pass before rules for AI systems—which are integrated into regulated products—apply. The Commission has initiated the AI Pact, a voluntary initiative aimed at supporting the future implementation and inviting AI developers from Europe and beyond to adhere to the main requirements of the AI Act ahead of time, in order to ease the transition to the new regulatory framework.[27]

[27] *EU AI Act: first regulation on artificial intelligence*, European Parliament (June 8, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

CHAPTER 6
CONCLUSION AND SUGGESTIONS

6.1 CONCLUSION

AI-related privacy concerns are a fundamental issue that needs to be carefully considered. AI systems' capabilities grow along with those of computer systems. Any kind of privacy violation is also against democratic principles and human rights. Since artificial intelligence (AI) is the product of the fusion of various domains with the goal of creating something superior to its parts, it is challenging to assess the risk of privacy violation in the context of AI due to the field's adaptive and evolutionary nature.

Each system component must be taken into account independently in respect to privacy contexts in order to protect privacy in AI systems. Privacy risks are prevalent in knowledge representations, natural language processing (NLP), automated reasoning, and the development, application, and use of machine learning models in the state of AI today. The challenge of addressing privacy risks in AI systems is one that will only get harder as the technology advances. As a result, ongoing evaluation of the ways in which individual technologies in an AI system interact with one another and contribute to privacy risk will be beneficial for future research in the field of privacy in AI.[28]

A lot of the urgent issues surrounding consumer privacy and data security are likely to change as a result of artificial intelligence and other data technologies. Important questions come up, such as whether we should step up government regulation or keep letting the market grow under the rules that are currently in place?

When customers want convenience and privacy at the same time, how do businesses decide on technology and data policies? How do we strike a balance between the additional risk that artificial intelligence (AI) poses to data security and privacy? Should legislators be forced to take action, will we allow local governments to make mistakes along the way or will we demand national federal legislation? Will we rely on the courts to interpret current laws on an individual basis, or will we wait for new laws to close persistent gaps? It is important that researchers from a variety of fields, such as economics, computer science, and law, science, statistics, and marketing.

Al and autonomous robots pose an existential threat to humanity, according to some scientists, philosophers, and futurologists. That's not how far we go. However, it appears that Al's actions will have a significant impact on democratic institutions and constitutional rights. Al may not require our intervention, but we will undoubtedly need to be vigilant.

The emergence of artificial intelligence (AI) technologies at the start of the twenty-first century has

[28] H Wang, *Human-in-the-Loop Person Re-Identification*, Proc. Eur. Conf. Comput 405-422 (2016).

brought about a new era of ease, innovation, and efficiency never seen before. Artificial Intelligence (AI) has permeated every aspect of our daily lives, from self-driving cars to virtual personal assistants, from recommendation engines to medical diagnostics. However, along with these incredible developments comes a pressing issue that has drawn the interest of people, institutions, and governments: preserving privacy in the era of artificial intelligence worldwide.

6.2 SUGGESTIONS

It is crucial that AI technology be subject to efficient regulation and oversight in order to guarantee that it is developed and used in a way that respects individual rights and freedoms. This covers not just how AI systems gather and use data, but also how these systems are designed and developed to be open, understandable, and impartial.

Governments, business, and civil society will need to work together to develop precise standards and guidelines for ethical usage of AI in order to effectively regulate this technology. To make sure that these requirements are met, there will also need to be constant oversight and enforcement.

In the absence of appropriate regulation, there is a chance that the growing application of AI technology will worsen already-existing biases and inequalities in society, as well as further erode civil liberties and privacy. We can ensure that this potent technology is used for the greater good while preserving individual liberties and rights by putting in place a regulatory framework for AI.