Global Scientific JOURNALS

GSJ: Volume 11, Issue 5, May 2023, Online: ISSN 2320-9186

www.globalscientificjournal.com

DATA PRIVACY CONSIDERATION IN ARTIFICIAL INTELLIGENCE (AI)

Tazanu Ateawung Elijah

Abstract

The role and place of technology in our contemporary society is one which cannot be over-emphasized. This is because it is res ipsa loquitur (the thing speaks for itself). AI is fast taking over the world to the point where it touches almost every domain of human life. This expedient growth of AI is one which is characterized with both positive and negative impacts in the society at large. This justifies why AI creators and other tech personnels have warned on the usage of AI. AI has considerable adverse effects on data privacy. One cannot remain indifferent to the adverse of AI on data privacy and consequently, it is a serious call for concern. This present article seeks to expose the adverse effects of AI on data privacy and possible recommendations.

Key words: Artificial Intelligence and data privacy

BACKGROUND TO THE STUDY

The Industrial Revolution was a turning point in the evolution of the society and it was difficult to predict to what extent the revolution will affect the world at large. The evolution of the society after the Industrial revolution came with several changes and innovations, all geared towards the development. Technological growth has been exponential in so far as these changes are concerned, eventually leading to the creation or emergence of Artificial Intelligence.

Evolution of AI and Data Privacy

Both concepts have not always existed and have seen the light owing to the evolution of the society. Consequently, they are quite recent in nature. In the subsequent paragraphs, we will briefly elaborate on the evolution of AI and Data Privacy

Evolution of AI

Artificial Intelligence dates back to early efforts in the 20th Century in building artificial neural networks (brain networks) to replace the human intelligence, which can be considered as the ability to learn and interpret from the information[1]. It was originally fashioned to understand the neuron activity in the human brain[2]. AI was born as a result of these efforts, that is, as computer programs that can perform predefined tasks at speedier and more accurate rates. AI capabilities have developed to include computer programs expanded that can learn from vast amounts of data and make decisions without human guidance, commonly referred to as Machine-learning (ML) algorithms [3]. Earlier algorithms relied mainly on pre-programmed rules to execute tasks, meanwhile, machine learning algorithms are designed with rules about how to learn from data that involves inferential reasoning perception, classification and optimization to replicate human decision making[4]. Machine Learning-driven decisions are primarily dependent on the data rather than on pre-programmed rules and, thus, typically cannot be predicted well in advance[5].

The growth and development of AI is one which cannot be over emphasized for it is res ipsa loquitur[6].

Evolution of Data Privacy

It was only around the 20th century that 'data privacy' began to come into focus[7]. This was because data collection tools became more sophisticated, companies began to experiment with personal data collection in various forms, including mailing lists and collecting customer banking information[8]. There has been an increasing public awareness of the importance of data privacy, instigated by revelations from privacy advocates and regulators, and the general transition of our lives on the internet[9]. The fourth amendment of the constitution of the United States of America[10] is a typical example of infant consecration of privacy legislation in the world at large and particularly in the US. In the case of ***Katz vs. The United States,*** the

[1] Izenman, A. J. (2008). Modern multivariate statistical techniques. Regression, classification and manifold learning, 10, 978–0. Springer, New York, NY. (IN)
Araz Taeihagh (2021): Governance of artificial intelligence, Policy and Society,
DOI: 10.1080/14494035.2021.1928377
https://doi.org/10.1080/14494035.2021.1928377

[2] ibid

[3] Ibid

[4] Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation.
Harvard Journal of Law & Technology, 31(2), 889 (IN) Araz Taeihagh (2021): Governance of artificial intelligence, Policy and Society,
DOI: 10.1080/14494035.2021.1928377
https://doi.org/10.1080/14494035.2021.1928377

[5] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679

[6] The thing speaks for itself

[7] Robin Andruss, A Brief History of "Data Privacy "and what lies ahead, (https://www.skyflow.com/post/a-brief-history-of-data-privacy-and-what-lies-ahead) June 27 2022, consulted 25/04/2023

[8] Ibid

[9] Ibid

[10] which became law in 1789 and forbids illegal search and seizure of people's property by the government

US Supreme Court ruled that Katz was entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was unnecessary to bring the Amendment into play. "The, the Fourth Amendment protects people, not places," wrote Justice Potter Stewart for the Court.[11] "

It is therefore prime and of utmost essence to define both concepts of AI and Data Protection

Definition of Artificial Intelligence and Data Privacy

Definition of AI

The polemics as a result of the broad and complex nature surrounding the concept of Artificial Intelligence has made it very difficult to arrive at a universally accepted definition. However, scholars have defined AI in the subsequent ways;

Artificial intelligence is defined as a science that aims to understand the nature of human intelligence through the work of a computer program, and the ability to simulate intelligent human behavior, and it means the ability of a computer program to solve a problem, or make a decision in a situation, that is, the program itself Finds the method that should be followed to solve the issue or reach a decision to identify the similarities between different situations and adapt to emerging situations[12].

John McCarthy originally defined Artificial Intelligence as “the engineering and science of producing machine intelligence”[13].

Areas of Artificial Intelligence

The scope of application of Artificial Intelligence is quite vast, touching almost almost every domain of life. These areas of AI will be examined in the subsequent paragraphs.

Understanding Language: It has the ability to "understand" and respond to the natural language, translates from spoken language to a written form and to translate from one natural language to another natural language. Speech understanding, Semantic Information

[11] "Katz v. United States." *Oyez*, www.oyez.org/cases/1967/35. Accessed 25 Apr. 2023.

[12] Jamal bin Subaih Al-Hamlan Al-Sharari, The Impact of Artificial Intelligence on the Quality of Administrative Decision from the Point of View of Secondary School Leaders in Al-Jouf Educational Region, Volume 8, Part 1, Solouk Magazine, Ibn Badis University Mostaganem, Algeria, 2021, pp. 18-19.

[13] International Journal of Interdisciplinary Educational Research, ISSN:2277-7881; IMPACT FACTOR :7.816(2022); IC VALUE:5.16; ISI VALUE:2.286, www.ijmer.in Digital Certificate of Publication: http://ijmer.in/pdf/e-Certificate%20of%20Publication-IJMER.pdf

Processing (Computational Linguistics), Question Answering, Information Retrieval Language Translation[14], are all features of understanding language.

Learning and adaptive systems: It has the ability to adapt behavior based on previous experience, and develop general rules concerning the world based on such experience. Here we focus on Cybernetics and Concept Formation[15].

Problem solving: It has the ability to formulate a problem in a suitable manner, plan for its solution and know when new information is needed and how to obtain such information. The components of problem solving are Inference (Resolution-Based Theorem Proving, Plausible Inference and Inductive Inference), Interactive Problem Solving, Automatic Program Writing, and Heuristic Search[16].

Perception (visual): It has the ability to analyse a sensed scene by relating it to an internal model which represents the perceiving organism's **"knowledge of the world."** The result of this analysis is a structured set of relationships between entities in the scene. Pattern Recognition and Scene Analysis[17] are elements of perception

Modeling: It has the ability to develop an internal representation and set of transformation rules which can be used to predict the behavior and relationship between some set of real-world objects or entities:

The Representation Problem for Problem Solving Systems,Modeling Natural Systems (Economic, Sociological, Ecological, Biological etc.), Hobot World Modeling (Perceptual and Functional Representations)[18]

Games: It has the ability to accept a formal set of rules for games such as Chess, Go, Kalah, Checkers, etc., and to translate these rules into a representation or structure which allows problem-solving and learning abilities to be used in reaching an adequate level of performance[19].

Robots: it consists of most or all of the aforementioned abilities with the ability to move over terrain and manipulate objects, exploration, transport/Navigate, Industrial Automation (e.g., Process Control, Assembly Tasks, Executive Tasks), security, Other (agriculture, fishing, mining, sanitation, construction, etc.), military, and household[20] etc.

Definition of Data Privacy

[14] Avneet Pannu, M. Artificial Intelligence and its Application in Different Areas, International Journal of Engineering and Innovative Technology (IJEIT) Volume 4, Issue 10, April 2015, ISSN: 2277-3754, ISO 9001-2008

[15] Ibid

[16] Ibid

[17] Supra, note 7

[18] Ibid

[19] Ibid

[20] Supra, note 7

Data simply refers to information[21] privacy on the other hand refers to secrecy[22]. Therefore, Data Privacy also referred to as information privacy can be defined as an aspect of data protection that addresses the proper storage, access, retention, immutability and security of sensitive data[23]. Data privacy does not exist ex nihilo but rather it is a discipline that involves rules, practices, and tools, to help organizations establish and maintain required level of privacy compliance[24].

Impacts of AI on Data Privacy

Information Technology has had a significant impact on users' privacy as more personal information is collected, processed, shared, and disseminated. Disseminating and sharing personal information may put individuals' privacy at risk. How therefore can this situation be salvaged? Privacy is a multi-faced concept that comprises of certain information about users that is sensitive and consequently should be kept private. User's identities should be protected and user's actions should not be traceable[25]. The right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (ICCPR)[26]. Although not contained in the African Charter on Human and Peoples' Rights (ACHPR), the right to privacy of children is contained in article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC)[27]. Interestingly, in 2017, the Supreme Court of India declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, and as part of the fundamental freedoms guaranteed by Part III of the Constitution of India[28].

The online DVD delivery service Netflix, in 2006 started a competition for improving its movie recommendation system based on users' previous ratings. To this effect, Netflix

[21] "Data." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/data. Accessed 26 Apr. 2023.
factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation

[22] "Privacy." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/privacy. Accessed 26 Apr. 2023.
freedom from unauthorized intrusion **:** state of being let alone and able to keep certain especially personal matters to oneself

[23] **Stephen J. Bigelow,** data privacy (information privacy), https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy. accessed on the 26 April 2023

[24] Ibid

[25] SABRINA DE CAPITANI DI VIMERCATI, SARA FORESTI, GIOVANNI LIVRAGA and PIERANGELA SAMARATI∗, DATA PRIVACY: DEFINITIONS AND TECHNIQUES, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems Vol. 20, No. 6 (2012) 793–817 c World Scientific Publishing Company, DOI: 10.1142/S0218488512400247

[26] ICCPR, article 17 "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
(2) Everyone has the right to the protection of the law against such interference or attacks."

[27] (ACRWC), article 10 "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."

[28] Justice K.S. Puttaswamy and Another v Union of India and Others, Petition No. 494/2012, 24 August 2017 (accessible at: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug2017.pdf).

released 100 million records about movie ratings by 500,000 of its subscribers. The released records were de-identified substituting subscribers' personal identifying information (e.g. name and IP address) with numerical user IDs. However, by linking the movie recommendations available on the Internet Movie Database (IMDb) with the de-identified Netflix dataset, it was possible to re-identify individuals, thus revealing potentially sensitive information. For example, a homosexual mother sought damages in a lawsuit for being outed by Netflix released data[29].

Privacy management is major concern under AI as at now and as predicted by some researches, will still constitute a problem in the next decade[30]. In a digital age like ours today AI is indispensable in our contemporary societies and consequently, is a call for serious major concerns. AI mechanisms present in people's homes will be privy to intensively private moments such as bathing and dressing[31]. The president of Microsoft recently remarked that:

"[Intelligent 3] technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression. These issues heighten responsibility for tech companies that create these products. In our view, they also call for thoughtful government regulation and for the development of norms around acceptable uses."[32]

One way in which AI is already affecting privacy is via Intelligent Personal Assistants (IPA) such as Amazon's Echo, Google's Home and Apple's Siri. These voice activated devices are capable of learning the interests and behaviour of their users. The concerns raised are about the fact that they are always on and listening in the background other than what is requested of these devices. In as much as these devices are designed to respond only to that which is requested of them, one cannot actually control the amount of information they receive other than that which is expressly provided to them by their users[33].

Digital technologies in general and AI in particular can have desired and undesired effects. Therefore a regulatory framework is of prime essence and indispensable. Luciano Floridi describes 'governance of the digital' as follows:

"Digital Governance is the practice of establishing and implementing policies, procedures and standards for the proper development, use and management of the infosphere. It is also a matter of convention and good coordination, sometimes neither moral nor immoral, neither

[29] Supra, note 25
A. Narayanan and V. Shmatikov, Robust de-anonymization of large sparse datasets, in Proc. IEEE S&P 2008, Berkeley/Oakland, CA, USA, May 2008.
[30] Eleanor Bird, Jasmin Fox-Skelly, Nicola Jenner, Ruth Larbey, Emma Weitkamp and Alan Winfield, The ethics of artificial intelligence: Issues and initiatives, PE 634.452, ISBN: 978-92-846-5799-5, doi: 10.2861/6644, QA-01-19-779-EN-N
http://www.europarl.europa.eu/stoa (STOA website)
[31] Ibid
[32] Ibid
[33] Ibid

legal nor illegal. For example, through digital governance, a government agency or a company may

(i) determine and control processes and methods used by data stewards and

data custodians in order to improve the data quality, reliability, access, security and availability of its services; and

(ii) devise effective procedures for decision-making and for the identification of accountabilities with respect to data-related processes”[34]

In 1983, the Court elaborated a ‘fundamental right to informational self-determination’ in response to the risks to the protection of the right of privacy that were associated with emerging digitization[35]. In 2008 the Court took the innovative step of extending the reach of fundamental rights protection to the fundamental right to the guarantee of the confidentiality and integrity of information technology systems[36]. The Court later held in 2016 that the protection afforded to information technology systems covers more than simply the computers used by individuals but also includes the networking of those computers with other computers, such as in connection with storage of data in the cloud[37]. it emphasised that data that are stored on external servers with a legitimate expectation of confidentiality are also deserving protection. Protection is also granted where a user’s movements on the internet are tracked. As a result, the use of AI associated with such networks also may fall within the protective scope of this fundamental right[38].

“If we only put in regulations after something terrible has happened, it may be too late. . . . The AI may be in control at that point,” Musk said in an interview with Fox News host Tucker Carlson. “That’s definitely where things are headed. For sure[39]…”

Recommendations

- Strengthen AI regulation:

  Most countries in the world are still to adjust to the growing trend of AI reason why the regulation of AI at this point in time can still be considered weak. Over

[34] Floridi L (2018) Soft Ethics, the governance of the digital and the General Data Protection Regulation. Philos Trans Royal Soc A 376:20180081. https://doi.org/10.1098/rsta.2018.0081
(IN) Wolfgang Hoffmann-Riem, Artificial Intelligence as a Challenge for Law and Regulation, Springer Nature Switzerland AG 2020, (https://www.researchgate.net/publication/337653460)

[35] Wolfgang Hoffmann-Riem, Artificial Intelligence as a Challenge for Law and Regulation, Springer Nature Switzerland AG 2020, (https://www.researchgate.net/publication/337653460)

[36] Ibid

[37] Ibid

[38] Ibid

[39] Caroline Downey, Elon Musk Warns That Regulation Is Needed before AI Is ‘In Control’, https://www.nationalreview.com/news/elon-musk-warns-that-regulation-is-needed-before-ai-is-in-control/

127countries globally have passed AI regulations[40]. Sam Altam[41] testified before a US Senate committee that AI regulation is crucial. He said “"I think if this technology goes wrong, it can go quite wrong...we want to be vocal about that," "We want to work with the government to prevent that from happening."[42]

- Define ethical red lines

A transparent and legitimate process is needed to assess whether any applications of digital technologies should be ruled out or not, regardless of their potential benefits, because the risks they pose are quite enormous and not proportionate to the benefits they procure. A typical example of such an application might be a lethal autonomous weapons system (“killer robot”[43]) in which killings are decided on by an algorithm[44]. This includes AI systems or applications that manipulate human behaviour to circumvent users’ free will (e.g. toys using voice assistance encouraging dangerous behaviour of minors) and systems that allow ‘social scoring’ by governments[45].

[40] Cathy Li, Global push to regulate artificial intelligence, plus other AI stories to read this month, 2nd May 2023 (https://www.weforum.org/agenda/2023/05/top-story-plus-other-ai-stories-to-read-this-month/#:~:text=Legislative%20bodies%20in%20127%20countries%20passed%20AI%2Drelated%20laws%20in%202022.&text=The%20European%20Commission%20proposed%20draft,risk%2C%20from%20low%20to%20unacceptable.) accessed on 25th May 2023

[41] CEO of OPEN AI

[42] James Clayton, Sam Altman: CEO of OpenAI calls for US to regulate artificial intelligence, 17th May 2023 (https://www.bbc.com/news/world-us-canada-65616866) accessed 25th May 2025

[43] Ray Acheson, A WILPF GUIDE TO KILLER ROBOTS, 3rd Ed. Women’s International League for Peace and Freedom, Jan 2020
Killer robots are autonomous weapon systems. These are weapons that operate without meaningful human control.

[44] Marie-Valentine Florin, Nine recommendations for the governance of AI systems, International Risk Governance Center, 28th Feb 2022

[45] Ibid