AI, CHATBOTS AND PRIVACY

Sahithi Aharam
School Of Computer Science And Engineering
VIT-AP UNIVERSITY
AMARAVATI-522237
INDIA
sahithi.21bce7896@vitapstudent.ac.in

ABSTRACT

The convergence of chatbots and privacy is a very common concern and new challenge for everyone in upcoming time. This paper explores the intersection of chatbots and privacy highlighting the laws that need to be introduced to protect the private data. We will go through the law, acts and bills that can be applied to safeguard our data. This paper concludes by giving the importance of introducing law that protects the privacy.

Keywords— Chatbots; Privacy; AI; Law

I. INTRODUCTION

Chatbots are software that is designed to interact majorly with a human. These chatbots use AI and NLP algorithms to help them to understand the query asked by humans and generate the responses to them just like a conversation between two humans. These are widely used in customer services, where they are used to solve the problems of customers without intervention from the company staff. Not only for customer services they are also used for various purposes such as providing information such as directions, finding local shops and restaurants, giving time weather, and general customer service. Chatbots usually respond to questions through text input, audio input, or sometimes even both. The usage of chatbots is growing fast, and they are becoming increasingly sophisticated. As they are becoming more popular, there are growing concerns about their impact on privacy. Chatbots collect a lot of data about their users, including their personal information and browsing history. This can track the user's behaviour, target them with advertising, and even manipulate them, so there is an immediate need for new privacy laws and regulations to protect users from the potential risks of chatbots. These laws should make sure that users have control over their personal data. The future of privacy is uncertain, but is visible that chatbots are going to play a huge role in that. It is important to make sure that chatbots are used in an ethical and responsible way.

The evolution of chatbots with advances in artificial intelligence (AI)

Chatbots have been around for decades, but they have only recently become popular, this is because of the advances in artificial intelligence that have made it possible to create chatbots that are more intelligent and engaging. The first chatbot was introduced in the year 1966 by Joseph Weizenbaum. He named the first chatbot Eliza. Eliza used pattern matching and substitution to stimulate conversation. It was intended to mimic human conversation by responding to user input with canned phrases and responses that were selected based on the patterns of the user's input. Inspired by ELIZA, Richard Wallace created a chatbot named Alice (Artificial Linguistic Internet Computer Entity) in 1995. Alice uses natural language processing to have conversations with humans. It is one of the strongest algorithms of its type and has won the Loebner Prize, which is awarded to accomplished humanoid, talking robots for conversation with humans. In 2000 a company developed a chatbot named smarter child, it was one of the first chatbots to become popular on instant messaging platforms, and it was available on instant messenger and Yahoo. Siri was developed by Apple for iOS in 2010. It is an intelligent personal assistant that uses a natural language user interface (UI). Siri is able to understand and respond to spoken commands, and it can perform a variety of tasks, such as setting alarms, making calls, and sending messages. Siri is considered to be one of the most popular and successful chatbots in the world. The present chatbot that is being used widely is ChatGPT (chat Generative Pre-Trained Transformer) which was developed by OpenAI. Primarily People had mixed opinions on chatbots but as time passed they are being worldwide.

The privacy risks associated with chatbots

Chatbots can collect a lot of data about their users when they search for information.It may collect data that includes personal information, such as names, addresses, and phone numbers, also user behavior, such as what websites they visit and what products they buy. This can be used to track users, target them with advertising, and even manipulate them. When comes to privacy risk the two main categories of security issues are threats and vulnerabilities. [1]A security threat is a risk by which an organization and its systems can be comprised, they can be spoofing, tampering, repudiation, information disclosure, etc. Threats to chatbots are isolated incidents that have the potential to cause harm to the data of the user. On the other hand system vulnerabilities are the weakness of a system that are exploited by hackers because of poor coding, lack of protection, weak firewall, and so forth. Human errors cause are the major reason for this issue. So we need to be careful when we provide our information to any chatbot.

II. LAW RELATED TO PRIVACY

Chatbots are becoming increasingly popular in India. They are being used in various sectors such as education, business, and entertainment, etc. However there are no particular laws or articles that are particularly applicable to chatbots but there are a few articles that that could be interpreted to apply to these issues. These include freedom of speech and expression[2], right against self-incrimination[3], protection of life and, personal liberty[4] . Furthermore to the articles, there are some acts and bills in India that could apply to privacy and chatbots. These include the Information Technology Act of 2000, and the Digital Personal Data Protection Bill of 2022. Interpretation of these articles and laws is still evolving. By using these laws, acts a person can protect himself from the theft of stealing data. These articles will discuss the legal implications of privacy and chatbots.

Article 19

Article 19(1)(a) of the Constitution of India guarantees the freedom of speech and expression to all citizens. This article speaks about liberty of one's speech and expression, it is a fundamental right that a person need to express their views without fear. This article applies in terms of chatbots because they should be free express their thoughts and ideas to chatbots that may include their political view, religious view, artistic view and personal view. These can be restricted in few situations for the protection of national security, public order. For example, a chatbot that is used by a government agency to provide customer service may be restricted from expressing political views and in the same way a chatbot that is used by a private company to provide entertainment may not be restricted from expressing political views.

Article -20

Article 20(3) of the Constitution of India provides a crucial safeguard for individuals accused of an offense. It enshrines the principle that no person who is facing criminal charges can be forced to provide evidence or testimony that would incriminate themselves. This constitutional provision is often referred to as the "right against self-incrimination" or the "privilege against self-incrimination. This right is essential for the protection of privacy, as it prevents the government from forcing people to reveal personal information that they would rather keep private. This article can be related in terms of chatbots because a person could request that chatbot to delete any personal information it collected. Even a person can refuse to answer questions from a chatbot that could incriminate them and can use a chatbot to communicate with others without revealing their identity.

Article 21

Article 21 of the Constitution of India, which guarantees the protection of an individual's right to life and personal liberty. The right to life and personal liberty is an important right because it ensures that everyone is treated fairly and justly by the government. It also protects individuals from arbitrary actions by the government or authorities. This article means that people have the right to control their personal information and prevent others from collecting or using it without their consent. A person at any

[1]Chatbots have indeed gained popularity across various platforms, but it's important for users to be aware of the potential security, privacy, and data protection concerns associated with their usage. Security: Chatbots can be used to collect personal information from users without their knowledge or consent. Privacy: Chatbots can be used to track user's activities and collect data about them. Data protection: Chatbots can be used to store and process sensitive data about users. Social: Chatbots can be used to spread misinformation or propaganda.

Manipulation: Chatbots can be used to manipulate or exploit users.

[2] The constitution of India, art.19

[3] The Constitution of India, art. 20.

[4] The Constitution of India, art. 21.

time can ask the chatbot to delete the information if it refuses they can file a case under Article 21. They can collect personal information such as phone number, email, and, current location, so it is important to be alert while providing the information.

Acts and Bills

Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is an Act of the Parliament of India that deals with the legal aspects of information technology.[5] It is an act that deals with cybercrime and electronic commerce. This bill was passed in the budget session of year the 2000. The first act that was passed in the year contained 94 sections, which was divided into 13 sections and 4 sections, after a few years third and fourth schedule was removed. The Information Technology Act (IT Act) is an important piece of legislation that regulates the use of information technology in India. It covers a wide range of topics, such as electronic signatures, digital signatures, data protection, and cyber security. The IT Act has helped to promote the growth of the IT industry in India and has made it easier for businesses to do business online. A Key provision of the IT Act is Section 67.[6] Section 67 of the Information Technology Act penalizes anyone who transmits obscene material that is lascivious in nature.

Digital Personal Data Protection Bill, 2022

The Digital Personal Data Protection (DPDP) Bill, 2022 was released by India's Ministry of Electronics and Information Technology (MeitY) on November 18, 2022.[7] This bill deals with personal data, data fiduciary, and processing. The principles include lawfulness, fairness, and transparency in that organizations must process personal data, organizations must limit their purpose of collecting data which is explicit, specific, and legitimate, and accountable for the data they have collected under The DPDP Bill. It also says about the right to be informed about the data that is being collected, the bill gives users the right to access the data they have provided to chatbots, and the right to request the removal of any information that chatbots have collected. It also establishes a Data Protection Authority (DPA) to oversee the implementation of the law, requires organizations to obtain consent from individuals before processing their personal data, and imposes penalties on organizations that violate the law.

III. KEY CASE STUDIES

The case of Bank of Baroda's chatbot: (2017)

In 2017, Bank of Baroda launched a chatbot called "Bank Baroda Chatbot" on Facebook Messenger. The chatbot was designed to provide customer service to Bank of Baroda customers.[8] However, the chatbot was found to be collecting personal

[5] The Information Technology Act, 2000 (Act 21 of 2000), s. 67.

[6] Section 67 of the IT Act prohibits the publication or transmission of obscene material in electronic form, with imprisonment up to 3 years and a fine of up to 5 lakh rupees.

[7] The Digital Personal Data Protection Bill is a proposed law that aims to protect the privacy of individuals' personal data in India. It defines personal data, sets rules for its collection, use, and sharing, and establishes a Data Protection Authority to oversee compliance.

[8] These are the types of chatbots that are introduced by Bank of Baroda

ADI: A chatbot that is available on the Bank of Baroda website and can answer questions about banking products and services, help with account enquiries, and provide customer support.

WhatsApp chatbot: A chatbot that is available on the WhatsApp messaging platform and can be used to answer questions about banking products and services, help with account enquiries, and provide customer support.

Facebook chatbot: A chatbot that is available on the Facebook social media platform and can be used to answer questions about banking products and services, help with account enquiries, and provide customer support. These chatbots are designed to provide customers with a convenient and efficient way to interact with the bank. They can be used to answer questions, get help with account enquiries, and even make transactions. The chatbots are still under development, but they are a valuable tool for customers who want to interact with the bank online.

information from users without their knowledge or consent violating articles 20, 21. This information included users' names, email addresses, phone numbers, and even financial information. The incident caused a backlash from users and privacy advocates. Bank of Baroda was forced to take the chatbot offline and apologize to its customers. The bank also promised to improve its privacy policies and to make sure that user's personal information was protected in the future. The case of Bank of Baroda's chatbot is a reminder of the potential privacy risks associated with chatbots.

The case of Google's Allo

In 2016, Google launched a messaging app called Allo. Allo was designed to be more private than other messaging apps, and it included several of features that were intended to protect users' privacy. For example, Allo used end-to-end encryption, which means that only the sender and receiver can know about the message. However, in 2017, it was revealed that Allo was collecting a wide range of personal information from users, including their location data, their contact information, and their browsing history. This information was being used by Google to improve the accuracy of Allo's predictions and to target users with advertising. The revelation that Allo was collecting so much personal information caused a backlash from users and privacy advocates. Google was forced to make changes to Allo's privacy settings, and the app was eventually discontinued in 2018. The case of Google's Allo is a reminder of the importance of privacy when using messaging apps. It is important to read the privacy policies of messaging apps carefully and to choose apps that respect your privacy.

IV. CHATBOTS AND PRIVACY

Chatbots have become increasingly prevalent in various online platforms, offering users a seamless and interactive experience. However, as the popularity of chatbots grows, so does the concern over privacy. One of the primary privacy issues associated with chatbots is the collection and storage of personal data. To function effectively, chatbots often require access to personal information, such as names, email addresses, and preferences, which users may share during interactions. Chatbots collect a variety of data from users, including personal information, transaction data, and interaction data. Ensuring the privacy and security of this data is essential to protect users from potential misuse or unauthorized access.[9] To address these concerns, developers and companies must implement robust privacy measures. This includes adopting data encryption techniques to safeguard sensitive information, limiting the storage of user data to the minimum required for the chatbot's functionality, and obtaining explicit consent from users before collecting and using their personal details. Furthermore, data should be anonymized and aggregated whenever possible to reduce the risk of individual identification. By incorporating these privacy safeguards, chatbots can maintain their valuable functionalities while respecting users' privacy rights. In addition to data privacy, transparency in chatbot operations is critical. Users should be made aware that they are interacting with a chatbot from the outset and provided with information about the data collection and usage practices. Clear and accessible privacy policies should be available to users, explaining how their information is handled and protected. Transparency builds trust between users and chatbot providers, ensuring that users feel comfortable engaging with the technology without fear of their privacy being compromised. Chatbots posing as legal websites are a growing threat to online privacy. These bots can trick users into entering sensitive personal information, such as credit card numbers or Social Security numbers, which can then be used to steal identities or commit fraud. If you are ever unsure about the authenticity of a chatbot, you can always contact the website or organization that the chatbot claims to represent directly. They will be able to verify the chatbot's identity and ensure that your personal information is safe.

V. FUTURE OF PRIVACY

The future of privacy is at a critical juncture, driven by rapid technological advancements and evolving societal norms. As data becomes increasingly valuable, individuals' personal information faces heightened risks. To secure privacy in the coming years, robust data protection measures must be embraced. This includes incorporating privacy by design principles into the development of new technologies, ensuring that privacy is considered from the outset. Additionally, the implementation of advanced encryption techniques and decentralized data storage solutions will enhance data security and reduce the risk of large-scale data breaches. Governments and regulatory bodies will play a crucial role in setting clear guidelines and enforcing privacy laws to hold companies accountable for mishandling personal data and ensure transparency in data collection and usage practices. Developers must adopt privacy-by-design principles, incorporating data encryption, anonymization, and secure storage practices to safeguard user data from unauthorized access or breaches. Additionally, advancements in AI and natural language processing will enable chatbots to better understand user intent without relying on personally identifiable information, promoting privacy-preserving interactions.

[9] Chatbots are becoming increasingly popular, but they also raise privacy concerns. Chatbots can collect personal information from users, such as their name, email address, and phone number. They can also track users' online activity and collect data about their interests. This data can be used to target users with advertising or to sell to third parties. Users should be aware of the privacy risks associated with chatbots and take steps to protect their personal information, such as only providing personal information to chatbots that they trust, being careful about what information they share with chatbots, and reading the terms of service and privacy policy of any chatbot they use.

Furthermore, user awareness and digital literacy will be pivotal in empowering individuals to protect their privacy effectively. Education on privacy best practices and the importance of informed consent will empower users to make informed decisions about their data. Privacy-focused tools and services will also become more common, giving users more control over their information. As technology continues to shape our lives, striking the right balance between innovation and privacy protection will be crucial for fostering trust in the digital environment and preserving individual liberties in the future.

VI. CONCLUSION

In conclusion, the rapid proliferation of chatbots presents both opportunities and challenges for the future of privacy. As these AI-powered conversational agents continue to evolve and integrate into various domains, protecting users' personal data becomes increasingly vital. They can be used to track your activities and to target you with advertising. Also can be used to manipulate you or to influence your behaviour. Be careful about the personal information that you provide to chatbots. Do not click on links or open attachments from chatbots that you do not trust. Use a privacy-focused browser extension, such as DuckDuckGo Privacy Essentials, to protect your privacy when browsing the web. Be aware of the terms and conditions of any chatbot that you use. Developers must prioritize privacy by implementing strong data protection measures, transparency, and user consent practices. Striking the right balance between personalization and privacy will be crucial in fostering user trust and acceptance of chatbot technology. Additionally, robust regulations and user education will play a pivotal role in shaping a privacy-centric future, ensuring that individuals' rights and data security are upheld in this dynamic digital landscape.

REFERENCES

[1] Adamopoulou, Eleni, and Lefteris Moussiades. "An overview of chatbot technology." In *IFIP international conference on artificial intelligence applications and innovations*, pp. 373-383. Springer, Cham, 2020.

[2] Rudolph, J., Tan, S., & Tan, S. (2023). War of the chatbots: Bard, Bing Chat, ChatGPT, Ernie and beyond. The new AI gold rush and its impact on higher education. *Journal of Applied Learning and Teaching*, *6*(1).

[3] Hasal, Martin, Jana Nowaková, Khalifa Ahmed Saghair, Hussam Abdulla, Václav Snášel, and Lidia Ogiela. "Chatbots: Security, privacy, data protection, and social aspects." *Concurrency and Computation: Practice and Experience* 33, no. 19 (2021): e6426

[4] Khosla, M. (2012). *The Indian Constitution*. Oxford University Press.

[5] Blythe, S. E. (2006). A critique of India's Information Technology Act and recommendations for improvement. *Syracuse J. Int'l L. & Com.*, *34*, 1.

[6] Singh, M., & Singh, A. K. Awareness and Protection Against Cyber Threats. *International Journal on Recent and Innovation Trends in Computing and Communication*, *2*(6), 1531-1534.

[7] Sundara, K., & Narendran, N. (2023). Protecting Digital Personal Data in India in 2023: Is the lite approach, the right approach?. *Computer Law Review International*, *24*(1), 9-16.

[8] Rani, R., Kanda, J., Chanchal, C., & Vij, T. S. (2023). A Study on Chatbots in the Indian Banking Sector. In *Contemporary Studies of Risks in Emerging Technology, Part A* (pp. 35-47). Emerald Publishing Limited