We are the products for sale in the age of AI.

P Rajagopal Tampi

Introduction

In the age of AI, knowingly, unknowingly, unwittingly, with or without consent, we are for sale. Yes, you and me. We are the products; AI is modelling us.

We know that passive listening is happening on our mobile phones, especially Siri, as anyone with an iPhone would have now experienced. Personal agents are marketed as discrete assistants which are supportive and simplify our lives. The Marketing story conceals that our most personal data is removed from our personal devices to the cloud for profiling and fine-tuning AI models of each one of us. The driver for this is the incessant quest for revenue growth and market share fuelled by heaps of cheap venture capital. Governments have not been able to block this undesired direction that AI has taken. Their failure to prevent personal profiling and AI modelling of citizens by regulations is glaringly obvious.

Training of personal agents and personal AI models

Training and using an AI model in today's AI age is so extremely easy due to the availability of algorithm libraries and LLMs. As a person with decades of IT experience, I can testify that the efforts, educational and programming capabilities required for training and deploying AI models has fallen by more than half compared to what was needed for software programming in the 1980s.

Personal agents track our thoughts through our actions, likes and dislikes preferences, priorities, whom and why we like to meet someone while avoiding another, our conversations and arguments with our family, work, associates, and social acquaintances. As individual models get fine-tuned on the cloud infrastructure of the product vendor based on personal data that the agent captures, accurate predictions of the thoughts and actions of the user will become possible. Combine this capability with your personal Adhaar and PAN numbers-based identification available to personal agents and what personal data is left to protect?

The Dangers

The danger lies in the models and data being sold for other purposes, including nefarious ones. Or the models may be misused by vendors who are lawfully entitled to use it for specific purposes or even hacked by criminals. Imagine that a company wanting to hire you buys or rents your AI profile model illegally for use-cases such as determining loyalty to the work organisation. You could lose the job opportunity based purely on that knowledge. Knowing your psychometric profile can result in impersonation to defraud and commit heinous crimes. Cloning can result in creating a legally identical duplicate identity or SIM card (for example), saddling citizens with losses, misfortune, and legal troubles.

Behind the curve

Unfortunately, data technologies available today do not support the advanced technological capability needed to monitor and prevent such harmful usage of personal AI models. Legal complexities and lack of clarity surround AI agents and AI entities. Nor are the laws maturing enough to decide on whether an agent is a juridicial person or not. We are not even sure of IP ownership of creations of art (for example) by AI.

Violations of the Law

Why is personal data of an individual allowed to be removed from the personal device to the vendor's cloud when Government and private company data are always processed on Government /company owned clouds? Is this not discrimination?

The removal of personal data from the individual's device for cloud-based processing violates the laws of most countries. Some examples are:

1. Fundamental rights guaranteed by Constitution of India, Justice K.S Puttaswami v. Union of India, AIR 2017 SC 4161, recognized the right to privacy as a fundamental right under Article 21 of the Constitution of India. The Supreme Court observed that “informational privacy” is a facet of the right to privacy, and that an individual has control over the dissemination of material which is personal to him. It further recognized the right of individuals to exclusively commercially exploit their identity and personal information, to control the information that is available about them online and to disseminate certain personal information for limited purposes alone.
2. Human rights guaranteed by United Nations Article 7 (discrimination), Article 12 (privacy and correspondence).
3. Data privacy rights guaranteed by GDPR under Article 22 of GDPR and Article 9.1 of GDPR which prevents “collection of data for the purpose of uniquely identifying a natural person”.
4. OECD AI principles of “non-discrimination, privacy and data protection, fairness, social justice.”

As additional references on the same subject of the ethics of personal agents you could refer to Wired and AIPathfinder.

Conclusion

Is it beneficial and fair to the individual to allow such personal profile data capture and its transfer to the cloud? Is individual person’s AI Modelling in the interest of that person? Who and what entities may be permitted to model citizens and for what purposes if any? What are the laws concerning the rights and standing of AI applications and AI derived Intellectual Property? These are some of the important questions which need answers in the short term.

The author recommends the solution which involves technology vendors processing all personal data on the personal device. Such a technology architecture is possible to develop and implement. It is a fair, legal, transparent and beneficial solution in the interest of individual citizens and society.

You may consider signing the change.org petition
Contact: Rajagopal.tampi@gmail.com

