Privacy Concerns and Legal Implications of AI tools like ChatGPT

Authors: Krishna CV Grandhi, Chandra Lekha

AI tools such as ChatGPT, Gemini, etc., use artificial intelligence to generate content, analyze data, and automate tasks. Their easy accessibility has made them popular for completing schoolwork, office tasks and also for seeking personal advice.

However, this widespread use has raised two major concerns: How well is the data shared being protected, and What could the possible legal consequences be upon a breach?

PRIVACY CONCERNS

1. **Inference Engines:** Every time a prompt is made, the AI learns from it, keeping a track of the information. Over time, it can link multiple prompts together and build an understanding of the individual's personal information such as their choices, habits and even sensitive information, without consent. AI tools can even use casual conversations to decode the personal information of the individual leading to breach of privacy.
2. **Training Model of AI:** AI models are trained on massive databases. Sometimes, personal data of individuals is included in these databases, intentionally or unintentionally. Even when collected with consent, it may later be used for a purpose that is beyond the consent given. This creates issues of trust and transparency, as people may feel misled if their data is being used without clear notice.
3. **Data leaks:** Companies, like OpenAI, have confirmed that user prompts are reviewed by a human moderator and flagged to the law enforcement in case any concerning activity is detected.

   In 2023, cybersecurity firm Group IB revealed that 26,802 ChatGPT accounts have been hacked and traded on the black market, with India having the highest record of 12,632 accounts.

   This highlights how vulnerable user data can be, and how it may easily be compromised.

LEGAL IMPLICATIONS

1. **Data Protection laws:** India has introduced the Digital Personal Data Protection Act, 2023, which aims to safeguard the personal data of individuals. However, it doesn't apply to data shared for personal or domestic purposes, meaning that if someone shares

information of personal concerns or issues with an AI tool, and that data is misused, they cannot claim protection under this Act. Similarly, the Consumer Protection Act, 2016 is not designed to handle complex AI-related issues.

This legal gap highlights the urgent need for a comprehensive AI-specific regulation.

2. **Mandating Explicit Consent:** When users disclose their data, many are unaware of how their data is collected, stored and reused.

   AI companies should be required to inform users about data handling practices before they share anything. Clear consent policies would not only fulfill legal obligations but also build user trust.

3. **Intellectual Property concerns:** Generative AI tools create works that mimic existing artistic styles, raising serious Intellectual Property issues. Recently, a trend had begun where a photo was converted into the Studio Ghibli art without seeking permission from the original creators of the art style. This raises the risk of infringing the original creators' copyright, as their style is replicated without consent or credit.

   The lack of clear laws governing AI generated content makes it difficult to decide liability, leaving a grey area in copyright law.

www.csail.org