AI systems such as ChatGPT could be violating users' privacy under GDPR, advocates worry

31 Mar 2023 | 12:59 GMT | **Insight**
By Lucy Valeski

Generative artificial intelligence systems such as OpenAI's ChatGPT could violate users' privacy under the EU's General Data Protection Regulation, a lawyer and a privacy advocate told MLex. But there isn't any relevant legal precedent for generative AI applications, which create content based on trawling swaths of data online, so it is tricky to determine what challenges companies might face from privacy watchdogs.

Generative artificial intelligence systems such as OpenAI's ChatGPT could violate users' privacy under the EU's General Data Protection Regulation, a lawyer and a privacy advocate told MLex.

But there isn't any relevant legal precedent for generative AI applications — which create new content, including text and images, from algorithms that find relationships between swaths of data online — so it is tricky to determine what challenges companies might face from privacy watchdogs.

ChatGPT, for example, takes data from all over the web and answers users' questions and demands with original content. Dall-E 2, also developed by US startup OpenAI, and Midjourney generate images based on users' written prompts and are trained on images and captions.

The implications for users' rights protected under the GDPR are unclear. The GDPR gives EU citizens the right to correct — or even delete — personal data concerning them held by companies, but privacy experts say it might be impossible to remove personal data from generative AIs' training models, whether it has been scraped from the Internet or gathered from user inputs.

"When it comes to highly advanced neural networks within programs that we call AI, the situation has changed because there isn't a specific piece of data that can be removed," Filip Konopczyński, a lawyer from privacy NGO Panoptykon said in an interview with MLex.

— Lack of precedent —

There are few cases of generative AI facing repercussions from data protection authorities.

Replika, a chatbot operated by a US company of the same name that created a "virtual friend" for users, was temporarily banned by Italy's data protection authority in February for not having necessary safeguards for children or checking users' ages (see here). Under Italian law implementing the GDPR, companies cannot process data of children under 14 without parental consent.

The Garante per la Protezione dei Dati Personali said that "the capability of 'Replika' to improve users' emotional wellbeing, help users understand their thoughts and alleviate anxiety through stress management, socialization and the search for love entails increased risks to individuals who have not yet grown up or else are emotionally vulnerable."

ChatGPT and other general chatbots don't establish a potentially emotional link with children, and OpenAI requires parental consent for users under 18, so those providers might not face this exact problem.

"The current issue is: we can think about the actual implications, but if there are no legal precedents, it is hard to say anything affirmatively," said Kris Shrishak, a technology fellow at the Irish Council for Civil Liberties, in an interview with MLex.

— Right to correction and deletion —

While many AI systems are trained on a specific data set for a specific purpose, ChatGPT and other generative AI technologies don't focus on any particular data. Instead, the software trawls the web and finds patterns to generate new content based on a prompt.

Shrishak said that people share information about themselves on the Internet in a specific context. If that information is used in the training of an AI model, it may be taken out of context, plus Internet users are unaware that their potentially personal data is being used.

“There is certain information that people have put out there in a very specific context,” Shrishak said. “When we use it for training purposes, you could lose that context.”

Another issue privacy advocates identified is that systems such as ChatGPT and Dall-E 2, which aren't based on application programming interfaces, train the model on user input. If someone enters personal data into these systems, the information enters the wide database of training data.

Under the GDPR, users have the right to remove or correct data under specific circumstances. But without a legal precedent, it isn’t clear whether or not users have the right to change or delete data in generative AI systems.

OpenAI says it lets users opt out of allowing their inputs on non-API systems, but they don't have a way to remove their data from the system without deleting an account.

Furthermore, it isn’t certain that companies will be able to locate information in their data set in order to change or delete it from the system.

It is “unclear if OpenAI knows how to get and receive information to correct or delete it,” Shrishak said.

— Coming up —

Data protection authorities' appetite to go after generative AI systems remains to be seen. Individuals could file a complaint that the system is breaking a law, or watchdogs could proactively impose consequences on these companies. However, the risk to privacy is relatively indirect.

In the meantime, Konopczyński said, companies could provide more transparency about how data is being used and accessed. They could also block users from searching people who aren't public figures so that individuals cannot see a compiled version of personal data lacking context about a private person.

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Related Portfolio(s):
Data Privacy & Security - European Commission's artificial intelligence strategy (EU)

Areas of Interest: Data Privacy & Security, Sector Regulation

Industries: Communication Services, Information Technology, Interactive Media & Services, Media, Media & Entertainment, Software and Services

Geographies: Europe, EU

Topics:

5G technologies | AI (Artificial Intelligence) | Big Data | Connected vehicles | Data localization | Data Privacy | Data transfers | Location-tracking | Future mobility