Legaltech® news

Four Key Privacy Risks to Consider Before Using Open Generative AI Systems
By Jessica Lipson
July 25, 2023

Most modern privacy laws implement the well-known privacy principles of transparency, purpose limitation, access, and security, among others. Here we analyze some of these principles and their application in the use of open generative AI systems.

It seems that every business is incorporating some form of generative artificial intelligence (AI) into their products and services, or thinking about how to do so. The technology is groundbreaking and may be able to increase productivity tremendously, but care must be taken in its use, as the technology poses many risks, including some very interesting privacy challenges, some of which we discuss in this article.

Most modern privacy laws implement the well-known privacy principles of transparency, purpose limitation, access, and security, among others. Let's analyze some of these principles and their application in the use of open generative AI systems.

Transparency

Under the GDPR the California Consumer Privacy Act, as amended (CCPA), and many other U.S. laws recently enacted, detailed disclosures must be given prior to or at time of data collection. These disclosures inform the individual whose data will be processed (let's call them the data subject) of what the business plans to do with their data, the purposes for such data processing, what data will be shared, with whom, and why such sharing occurs, among other things.

The challenge is that a business cannot provide a disclosure up front of what open AI platforms such as ChatGPT and Bard will do with the data once they have it. Once data sits in the neural network of a chatbot, it will be used for chatbot training, certainly, but may also be used to produce work product for another user. All of this is outside the business' control, and, indeed, the business has no visibility into what happens within that neural network. Therefore, any disclosures the business provides are necessarily going to be inadequate or potentially too broad to allow compliance with applicable laws.

Purpose Limitation

Under the GDPR and most newly enacted U.S. laws, personal information processing, use, sharing and retention must be reasonably necessary and proportionate to achieve the purposes for which the data was collected, as disclosed in advance to the data subject. As discussed, all data input to open AI platforms will be incorporated into and used by the chatbot in unpredictable ways. If subject to these laws, it would be impossible for a business to satisfy the legal requirement to limit the processing after the data is input into an open generative AI tool. That being the case, it is entirely possible that the business would need to treat this data sharing as a "sale" of the data, which brings with it several regulatory complications.

Access

The right of access takes different forms under different laws, but all seem to follow similar rules. Under the GDPR, for example, data subjects have the right to access their data (actually see what data the business collects about them, in detail), to rectify any inaccuracies in the data held by the business, to be forgotten (i.e., ask that their data be deleted entirely), to request that the business restrict the processing of their data to only specific uses, to request their data in a format that can be ported to another vendor, to object to processing of their certain sensitive data about them under certain circumstances, and to not be subject to automated decision-making.

The CCPA grants California consumers almost all these rights as well, as do most of the newly implemented U.S. state comprehensive privacy laws enacted in the past year or two (with some variation among laws, of course). When a business is responsible for data collection (they are a "controller," as many laws call this role, given that the business controls the collection and means of processing of data), they must honor these requests, to the extent there is no statutory exception that would permit them not to. There is no exception for processing of data using AI tools, and it may not be possible for a business to comply with all these requests made to it by the data subject when using them.

Security

All comprehensive privacy laws contain a requirement that the business must implement appropriate (or at least reasonable) controls to protect the personal data they collect and process, including when the processing is done by a service provider. Under some laws, such as the CCPA, the Attorney General has issued guidance that certain known frameworks will be considered reasonable, but anything less will not be.

Many businesses fall flat of this requirement today, particularly when, instead of auditing or verifying the security controls of their vendors, they assume compliance with all applicable requirements only because the vendor is reputable. We have already seen security breaches of several of the larger open AI chatbots available today, and the business would be remiss in their regulatory obligations if they used these chatbots without security verification first.

There are further requirements pursuant to many of these laws, including that the business conduct risk assessments to ensure that the risk of harm to the data subject does not outweigh the benefit to the business from the data processing (this one might be difficult to "pass" when using open AI tools), and that the business enter into agreements with other controllers of the personal data they process to govern such processing. There are myriad other requirements under both domestic and foreign privacy and data security laws which a business will find difficult to comply with, when inputting data into an open AI chatbot or allowing the chatbot to process such data. Care must be taken in the use of these technologies, which, while potentially deeply transformative, can lead to legal perils if improperly evaluated or used.

What can a business do to protect itself?

The first line of defense, as with all issues involving privacy, will be to engage risk, legal and governance teams, and the privacy officer to evaluate the risks associated with the processing early on, before beginning to use any AI tools. The second line of defense, in collaboration with risk, data and

The above article appeared in *Legaltech News* on July 25, 2023. Reprinted with permission.

governance teams, is to implement strong, and enforced, policies and procedures regarding use of open AI tools, including specific restrictions on the type of data that employees and contractors can input to the chatbots in use by the business. The business should restrict what personal data can be input into an open AI tool (or restrict it altogether, if the input cannot be done ethically, and in compliance with law).

Of course, login credentials for these tools might also allow identification of the employees who use them, and it would be advisable to create login credentials for business teams that do not in fact reflect any personal information of the individual users (e.g., select general logins that use strings of letters and numbers, or a department name, instead of a person's). When personal data must be processed by the AI chatbot, given the business need, consider closed systems that allow better control, and do not allow for business data to be incorporated into the AI tool's neural network used for its further training.

But in all circumstances, the business should always ensure that the risk, legal, governance and data teams are involved in all processing evaluations, so that, whatever the business decision is involving data processing, it is done taking all risks into consideration, including legal, ethical, safety, and public relations risks that might arise if the data were indeed misused by the AI tool or inappropriately disclosed.

Jessica Lipson is the co-chair of Morrison Cohen's Technology, Data & IP Department, with a focus on technology transactions, privacy and data security matters, and transactional intellectual property work.

The above article appeared in *Legaltech News* on July 25, 2023. Reprinted with permission.