What if you could automate all the work associated with interpreting rules and regulations that you must comply with as an organization? You could reduce your reliance on expensive consultants, former regulators, lawyers and maybe eliminate as much as 70% of the cost and effort.

At Innovation Factory (IF) we have been looking for a solution that would automate the time consuming and expensive effort of reading and interpreting rules and regulations related to data privacy. To test we decided to have ChatGPT, the latest AI tool, as a potential solution to interpret data privacy regulations and advise us what to do in the case of a data privacy breach.

Complying with data privacy regulations is crucial for a business to protect their customers' personal information, to avoid any legal/regulatory penalties, and maintain a strong reputation. "Would ChatGPT be a good source and useful tool for you to gather information on data privacy regulations and help guide your actions that you need to take to protect anyone impacted by such an event?". We randomly picked New Mexico's data privacy laws as the test case.

What we learned………

Inconsistent response:

One of the primary issues we discovered relying on ChatGPT for regulatory information was the unpredictability and inconsistency of the responses. We discovered that ChatGPT's responses can vary depending on the context of the question and the data it has been trained on, the user will also receive inconsistent responses to the same question asked differently or even asking the same question at a later point in time.

As an example, we asked ChatGPT how to comply with New Mexico's data privacy laws after a data breach occurs. In our test ChatGPT we asked the following question "I have a company in New Mexico. My company faced a data breach. I want to know whom all I should report to based on number of people affected in the breach". Chat GPT responded that the business must notify the New Mexico Attorney General when more than 250 people are affected.

However, when we asked the same exact question a few days later ChatGPT reverted back that if you have more than 100 people impacted you need to report to the New Mexico Attorney General within 45 days. Obviously, such inconsistencies would lead to confusion and non-compliance with actual regulations putting you at risk.

Not able to combine ChatGPT data sources with your internal data sources:

The ability to combine ChatGPT "regulatory information" with your own risk policies & procures is not possible. You might have developed a proprietary data protection framework (based on your risk appetite) that is unique to your business. Such proprietary knowledge is not accessible to ChatGPT or other public sources, making it difficult for businesses to combine and control the data sources making the recommendations from ChatGPT incomplete.

Inaccurate findings:

While ChatGPT strives to provide accurate and helpful responses to its users, there are also cases where it provided made-up or inaccurate regulatory information. Such inaccuracies would be harmful and can result in non-compliance with actual regulations, leading to legal and financial risks.

When we asked another question "I have a company in New Mexico. My company faced a data breach. I want to know whom all I should report to based on number of people affected in the breach" In this case, and the case above, ChatGPT provided a false response (response with a made-up regulatory obligation) stating that "the company needs to notify the Attorney General when more than 250 people are affected," while the number actually should be 1,000 (N.M. Stat. 57-12C-1 et seq.).

Conclusion:

While ChatGPT is easy to use and potentially can be a helpful tool for businesses to gather basic information on data privacy regulations, relying on their information can lead to unpredictability, inconsistency, and the risks of relying on "made-up" regulatory obligations.

I have no doubt that the tool will improve over time however, in my point of view it has too many deficiencies to be considered a serious solution for understanding and managing regulatory obligations.

Our Core Values: Best People | Respect for the Individual | Integrity | Stewardship | Client Value Creation

https://www.innovationfactoryllc.com/